SuperAP 570n

User Manual

October, 2012

Overview

The 570n 1 Watt AP/bridge offers excellent and reliable performance along with cost-effective point-to-multipoint outdoor and indoor wireless solutions perfectly suited for access technology, private networks and hotspots. The 570n works in the unlicensed 2.4 GHz Wi-Fi frequency band. It supports the newest IEEE 802.11n standard and is compatible with IEEE 802.11b/g, with options for SISO and MIMO functionality. The private protocol iPoll offers effective point-to-multipoint deployment scenarios.

Contents

1 Deployment Scenarios
- 1.1 HotSpot
- 1.2 Point to Multipoint
- 1.3 Light PTP

2 Initial Device Setup
- 2.1 Initial 570n Setup
- 2.2 Initial Station Setup

3 Operation Mode
- 3.1 Bridge Mode
- 3.2 Router Mode

4 General Device operation
- 4.1 Web Management Structure
- 4.2 570npling and Saving Configuration Changes

5 Configuration Guide
- 5.1 Status
    - 5.1.1 Information
    - 5.1.2 Network
    - 5.1.3 Wireless
    - 5.1.4 Routes
    - 5.1.5 ARP

- 5.2 Configuration

    - 5.2.1 Network
    - 5.2.2 Bridge Mode
    - 5.2.2.1 IPSettings
    - 5.2.2.2 VLAN to SSID Mapping
    - 5.2.2.3 Management VLAN

5.2.3 Router Mode
5.2.3.1 WAN Settings
5.2.3.2 LAN Settings
• 5.2.3.2.1 LAN DHCP Settings
5.2.4 Wireless
5.2.5 Wireless Mode: Access Point (auto WDS)
5.2.5.1 570n Basic Wireless Settings
5.2.5.2 570n Security Settings
5.2.5.3 570n Advanced Wireless Settings
5.2.6 Wireless Mode: Station
5.2.6.1 Station Basic Wireless Settings
5.2.6.2 Station Security Settings
5.2.6.3 Station Advanced Wireless Settings
5.2.7 Wireless Mode: iPoll Access Point
5.2.7.1 iPoll 570n Basic Wireless Settings
5.2.7.2 iPoll 570n Security Settings
5.2.7.3 iPoll 570n Advanced Wireless Settings
5.2.8 Wireless Mode: iPoll Station
5.2.8.1 iPoll Station Basic Wireless Settings
5.2.8.2 iPoll Station Security Settings
5.2.8.3 iPoll Station Advanced Wireless Settings
5.2.9 Virtual 570n
5.2.10 Wireless ACL
5.2.11 Traffic Shaping
5.2.11.1 Limit all traffic
5.2.11.2 Limit per IP traffic
5.2.12 Port Forwarding
5.2.13 Static Routes

♦ 5.3 Services

5.3.1 WNMS
5.3.2 System alerts
5.3.2.1 SNMP Traps Settings
5.3.2.2 SMTP Settings
5.3.3 SNMP Settings
· 5.3.3.1 Clock/NTP
5.3.4 SSH
5.3.5 HTTP

♦ 5.4 System

5.4.1 Administration
5.4.1.1 Device settings
5.4.1.2 Account settings
5.4.1.3 System functions
5.4.2 Log
5.4.3 LED Control
5.4.4 Firmware Upgrade

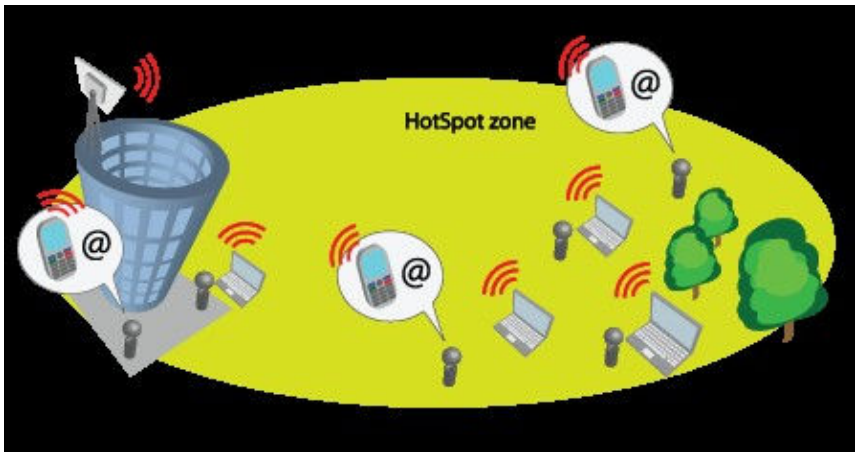
♦ 5.5 Tools
5.5.1 Antenna Alignment

5.5.2 Site Survey
5.5.3 Delayed Reboot
5.5.4 Ping
5.5.5 Traceroute
5.5.6 Spectrum Analyzer
♦ 6 UAM (Universal Access Method)
6.1 UAM Overview
6.2 UAM Configuration
6.3 White/Black List

Deployment Scenarios

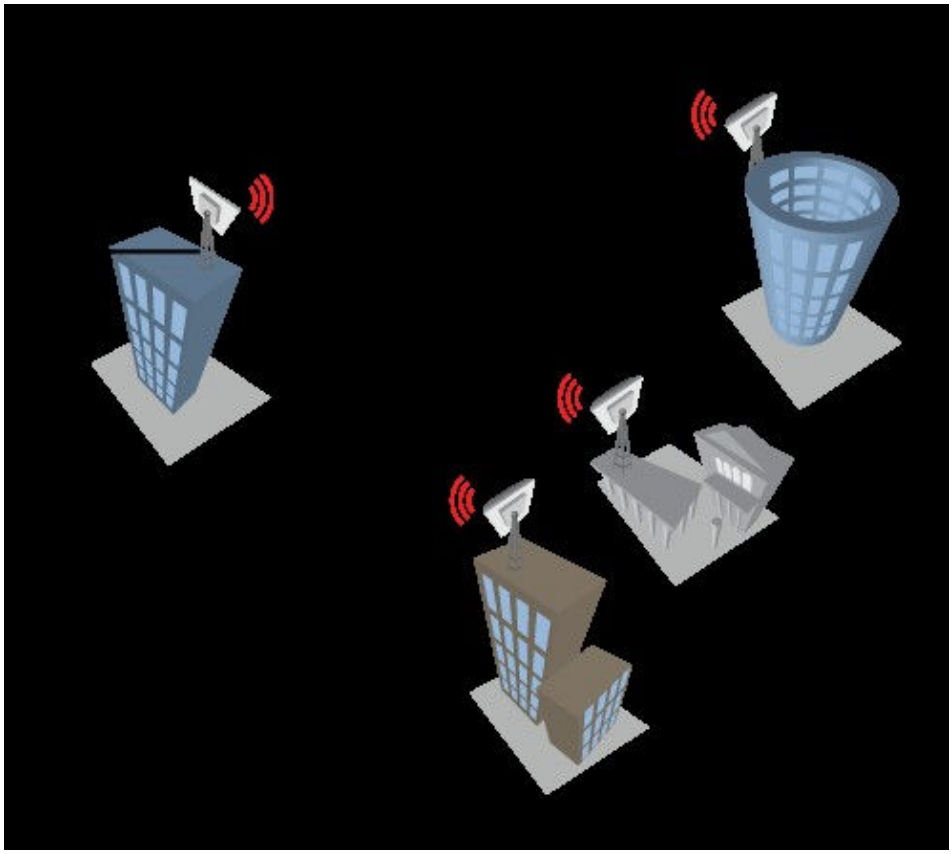
HotSpot

The 570n can easily create a hotspot network on the 2.4 GHz unlicensed band. IEEE 802.11n lets you achieve (depending on laptop, smart-phone or PDA capabilities) maximum throughput and supports all possible client equipment (based on IEEE 802.11b/g/n). Hotspot zones can be created indoor or outdoor. WLAN hotspots are very popular in hotels, MTU/MDU, hospitals, schools, government buildings, companies, and retail.



Point to Multipoint

IEEE 802.11n wireless multipoint which delivers several times higher throughput than 802.11a/g. The 570n supports a private wireless point to multipoint protocol called iPoll which allows connecting more than one iPoll Stations to the iPoll Access Point thus creating a robust point to multi point network.

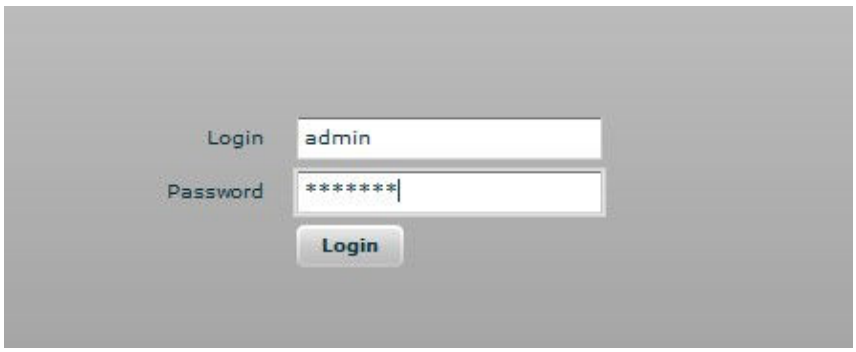


Light PTP

The 570n supports access point and station operating modes, therefore point-to-point can be created between AP and Station, or between 2 Stations, or between 2 APs. There are available options for SISO and MIMO antennas. Maximum achievable real data throughput is up to 160 Mbps.

Initial Device Setup

The default IP address is 192.168.2.66. To access the Web management interface, configure your PC with a static IP address on the 192.168.2.X subnet with mask 255.255.255.0. Connect the 570n device in to the same physical network as your PC. Open the Web browser and type the default IP address of the 570n device https://192.168.2.66/and the login page will be loaded. Enter default administrator login settings:



The default administrator login settings are:

Login: **admin**
Password: **admin01**

After successful administrator login you will see the main page of the device Web management interface. The device now is ready for configuration.

Initial 570n Setup

Follow the steps for initial wireless Access Point setup that will be prepared to accept wireless

Station connections (refer to the section Initial Station Setup for instructions).

1. Connect an Ethernet cable between your computer and the 570n.

2. Make sure your computer is set to the same subnet as the 570n, i.e. 192.168.2.150

3. Start your Web browser.

4. 570n uses following default settings:

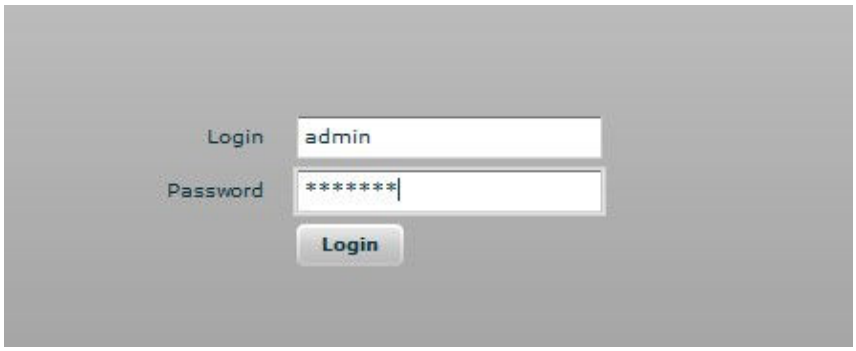
WAN IP: **192.168.2.66**

Subnet mask: **255.255.255.0**

Username: **admin**

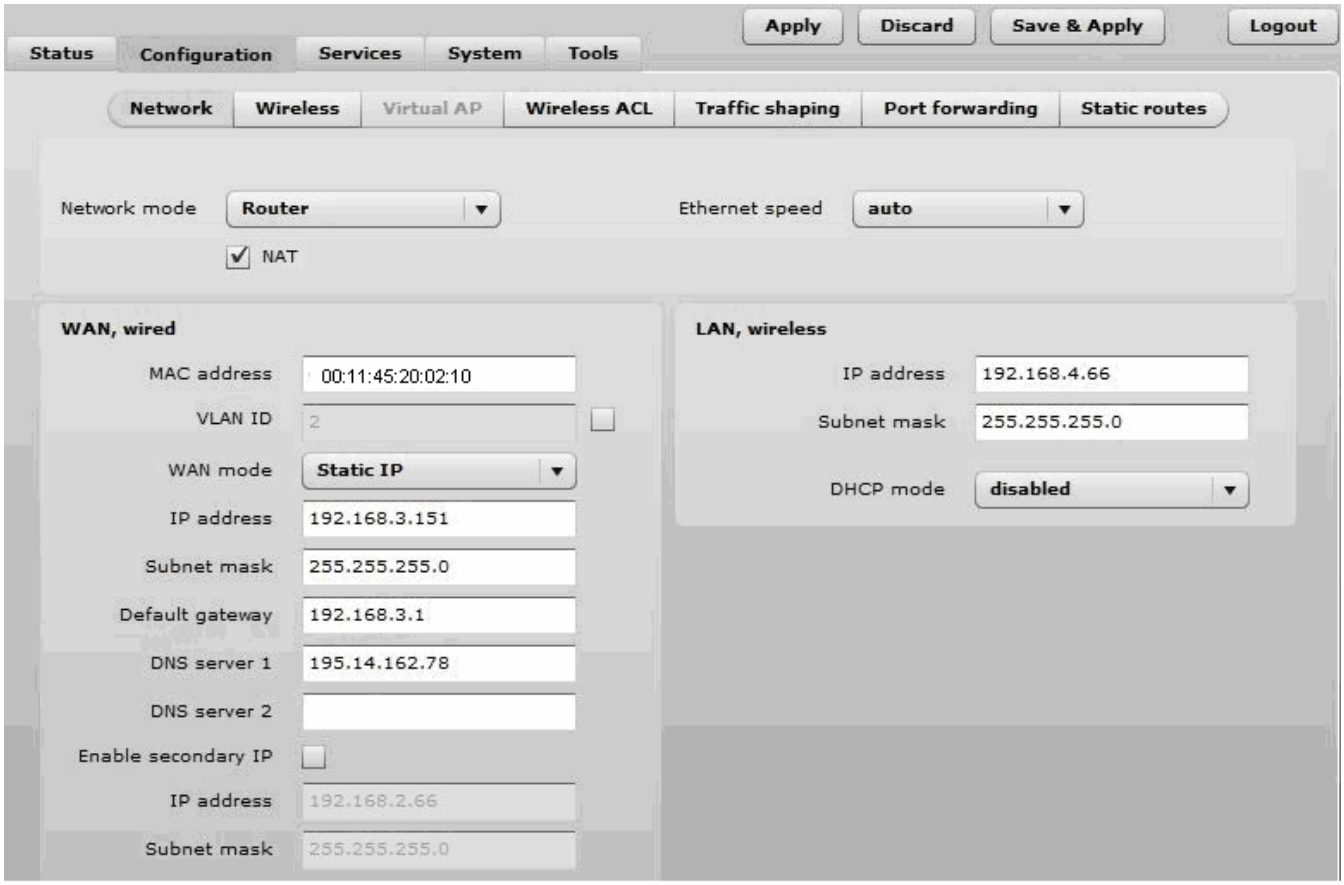
Password: **admin01**

The initial login screen looks as follow:

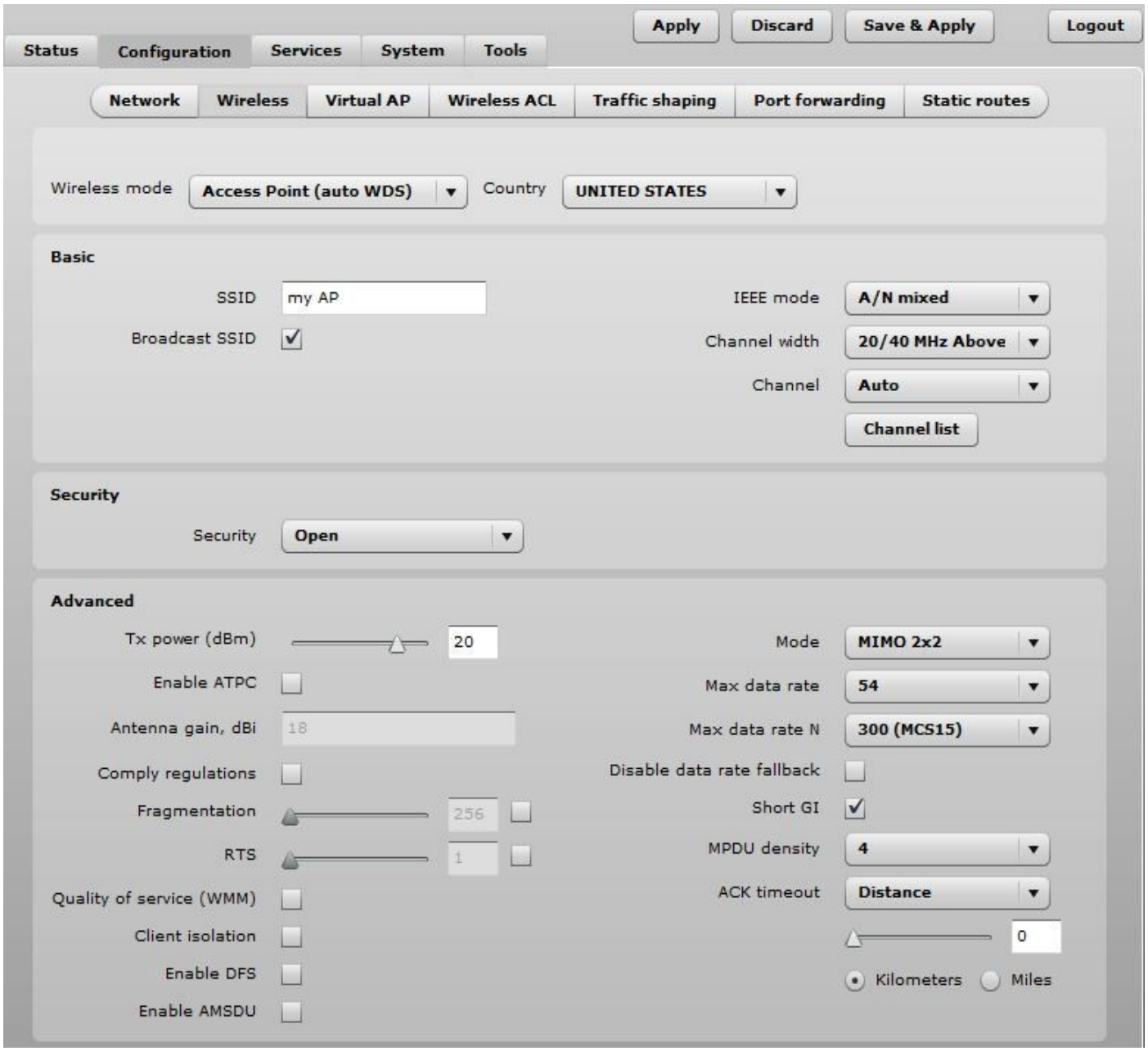


Step 5. Enter the default password, and then press the Login button to enter the 570n web management page.

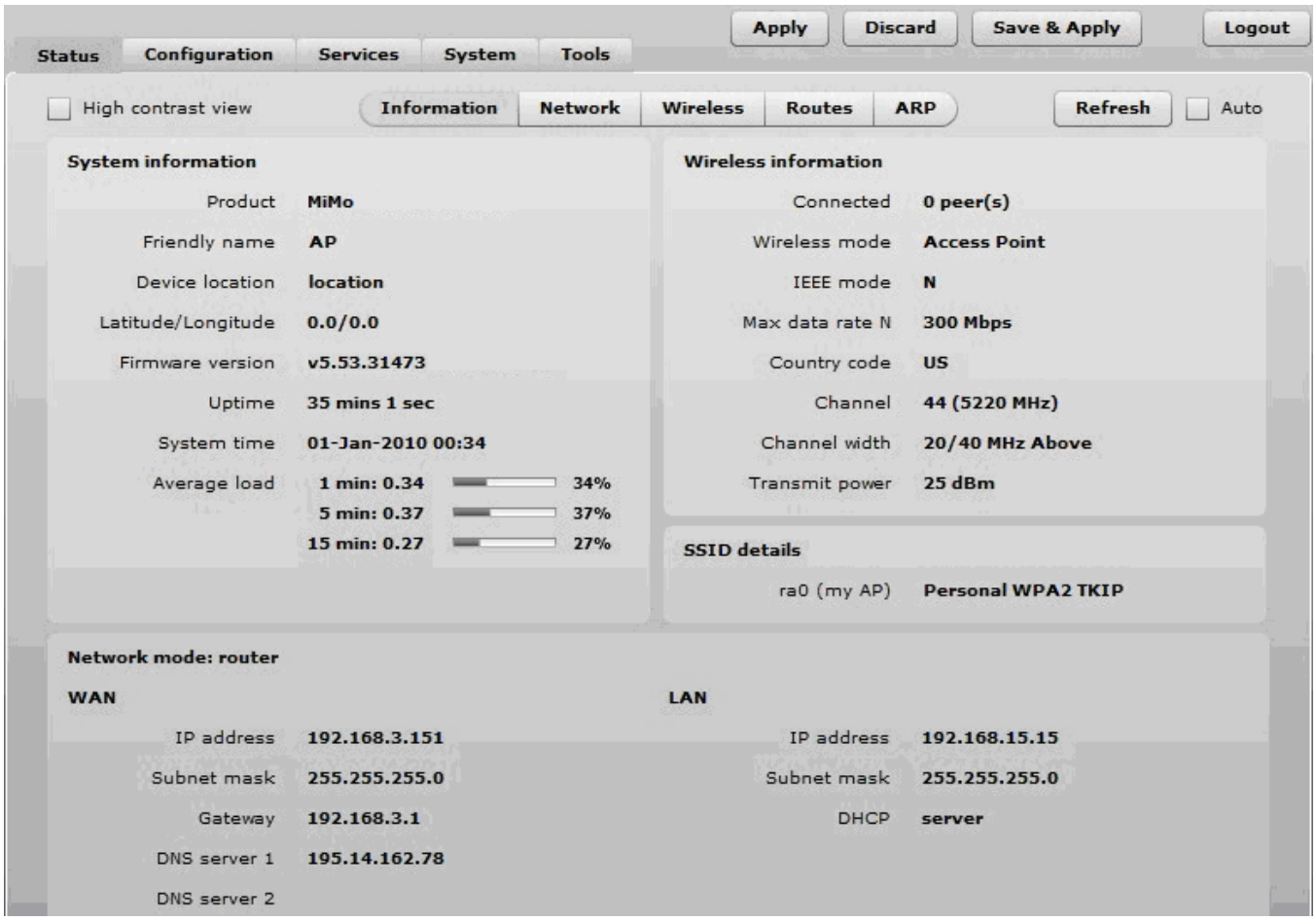
Step 6. Navigate to the **Configuration | Network** tab and choose the Router network mode with NAT enabled, Static IP enabled on WAN side, LAN settings with DHCP server enabled (to loan an IP addresses for connected clients) on LAN side and click **Save&Apply**:



Step 7. Navigate to the **Configuration | Wireless** tab, choose Access Point wireless mode with WDS enabled, specify the SSID with Broadcast enabled, Security parameters and IEEE mode and click **Save&Apply**:



Step 8. Verify connection. Navigate to **Status | Information** menu to check if the Station is successfully connected to the 570n device:



Initial Station Setup

Follow the steps for initial wireless client setup that will be connected to the previously configured 570n (refer to the section Initial 570n Setup).

Step 1. Connect an Ethernet cable between your computer and the 570n device.

Step 2. Make sure your computer is set to the same subnet as the 570n, i.e. 192.168.2.150

Step 3. Start your Web browser.

Step 4. Each 570n devices uses following default settings:

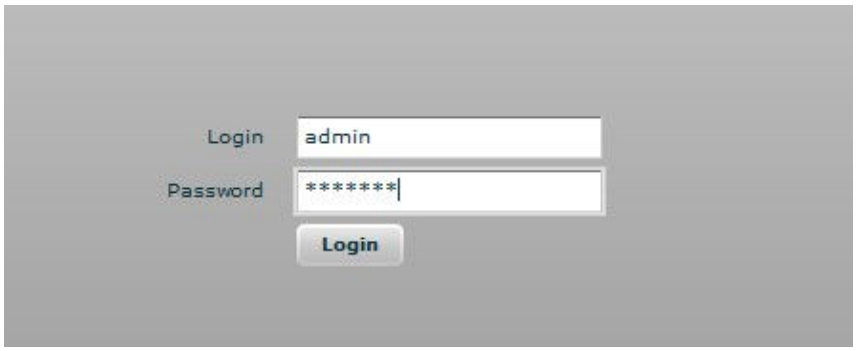
WAN IP: **192.168.2.66**

Subnet mask: **255.255.255.0**

Username: **admin**

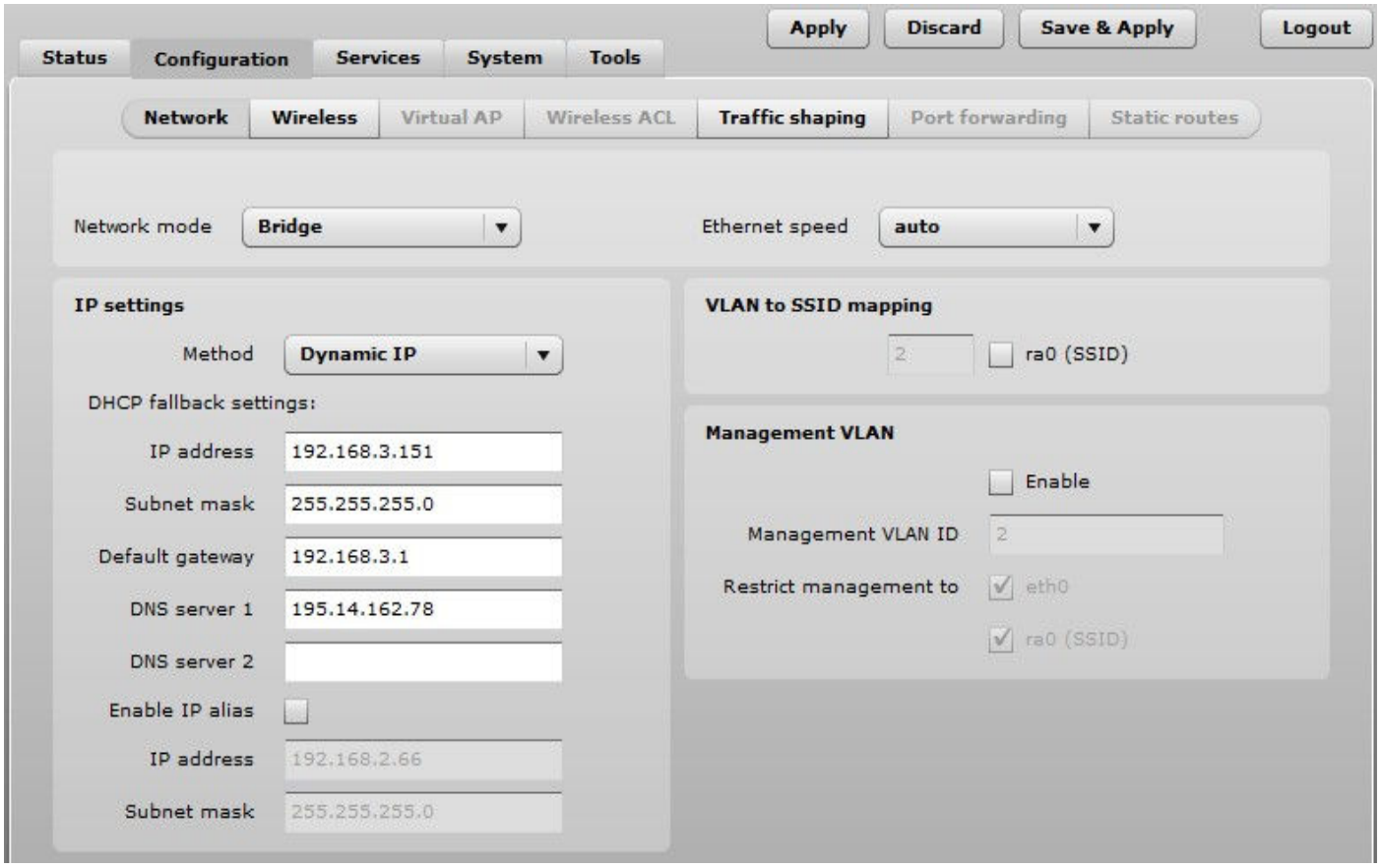
Password: **admin01**

The initial login screen looks as follow:

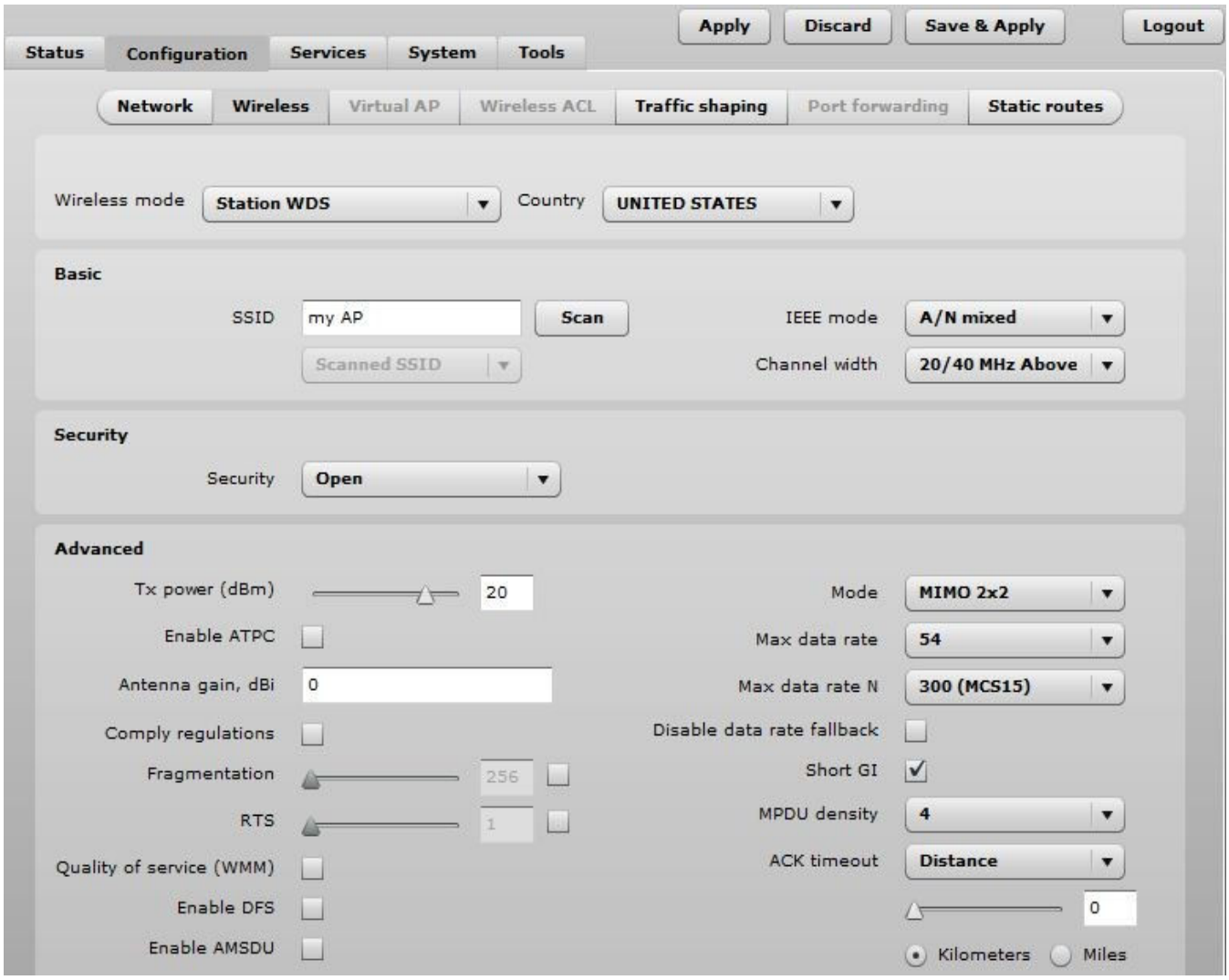


Step 5. Enter the default password, and then press the Login button to enter the 570n web management page.

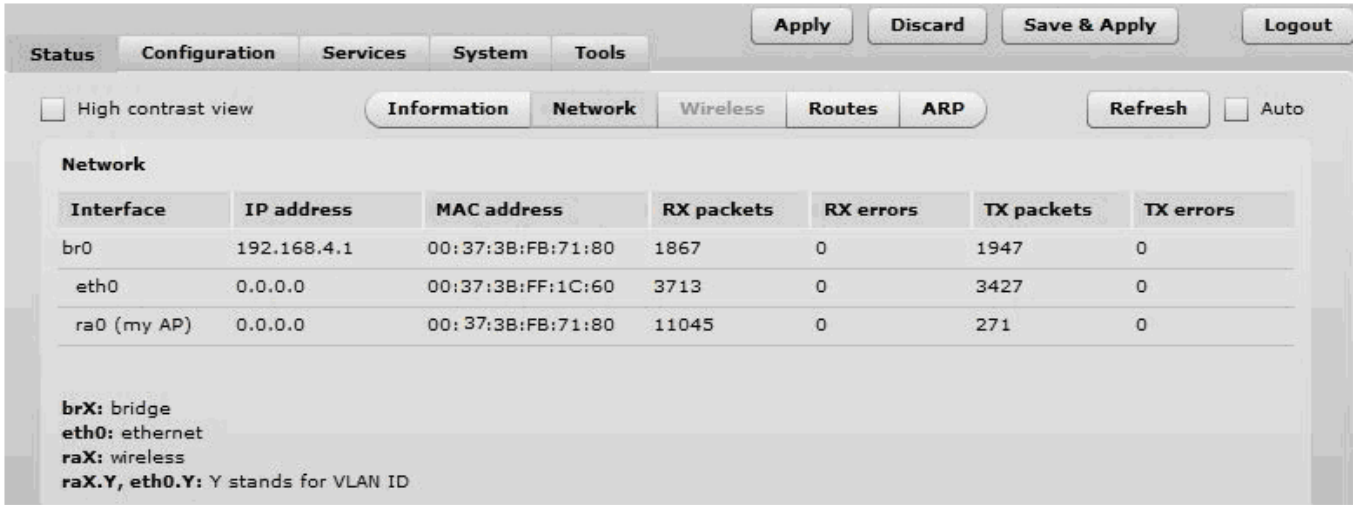
Step 6. Navigate to the **Configuration | Network** tab and choose the bridge network mode with, Dynamic IP enabled (be sure that 570n to which the device will be associated has a DHCP server running (refer to the section Initial 570n Setup for instructions), specify the DHCP fallback settings in case the DHCP server is unreachable and click **Save&Apply** button:



Step 7. Navigate to the **Configuration | Wireless** tab, choose Station WDS wireless mode, click **Scan** button near the SSID entry field to choose the SSID of the 570n where the station will be associated to. Specify the Security parameters for the 570n, check IEEE mode (these settings must conform with 570n wireless settings) and click **Save&Apply**:



Step 8. Verify connection. Navigate to the **Status | Network** page. The Network page will show main network information about association with 570n:



The main **Status | Information** page will display wireless information of the link with access point. The connection status must be displayed as Connected and progress bars indicating the quality of the connection must be displayed:

Operation Mode

The 570n device can operate as transparent Bridge or Router.

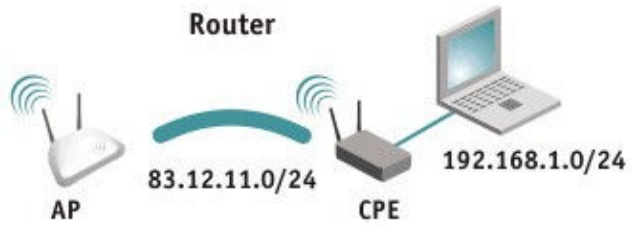
Bridge Mode

The 570n device can act as a wireless network bridge and establish wireless links with other 570ns. In this mode all LAN ports and Wireless interface will be a part of the Bridge.

With a Bridge, all connected computers are in the same network subnet. The only data that is allowed to cross the bridge is data that is being sent to a valid address on the other side of the bridge.

Router Mode

In router mode the 570n will receive internet through WAN port and will share it to the LAN ports that will be separated with a different IP range. The type of connection to the WAN interface can be made by Static IP, DHCP client or PPPoE.

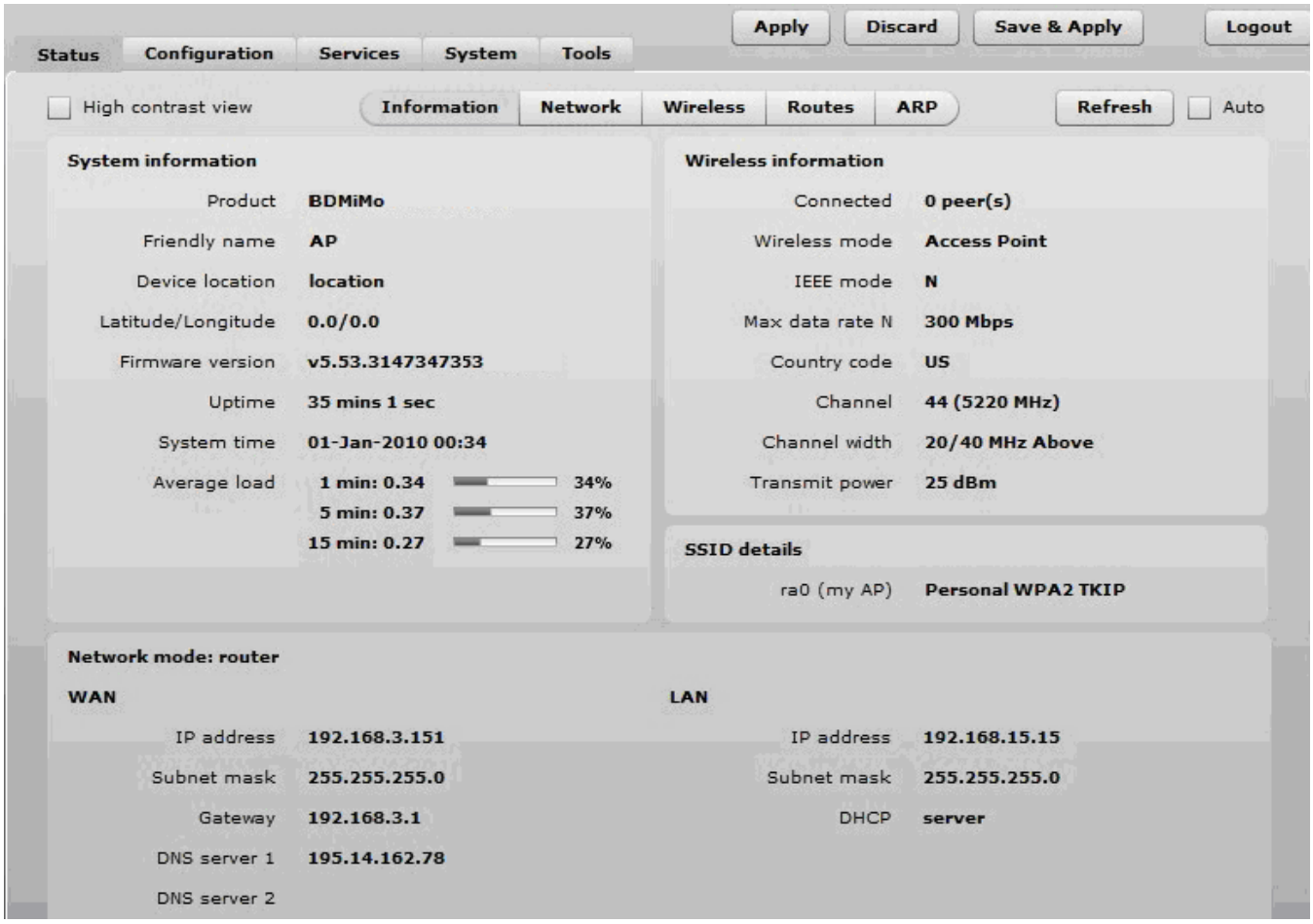


When device operates in Router mode, the traffic coming on wired interface and going out on wireless interface can be masqueraded by enabling NAT. NAT allows a set of clients to invisibly access the Internet via the 570n . To other clients on the Internet, all this outgoing traffic will appear to be from the 570n device itself.

General Device operation

Web Management Structure

The main web management menu is displayed after successfully login into the system (see the figure below). From this menu all essential configuration pages are accessed. The active menu tab is displayed in a different color:



By default the Status | Information menu is activated where the main device information is displayed. The 570n web management menu has the following structure:

Status

Information : displays general information of the device.

Network : displays main network and wireless statistics of the device.

Wireless : displays information about connected stations on the particular interface (only on station wireless mode).

Routes : displays unit's route table.

ARP : displays ARP table.

Configuration

Network : network mode, Ethernet speed, IP settings, management and data VLANs,

DHCP, PPPoE.

Wireless : specify wireless mode (AP, Station, iPoll AP, iPoll Station), country, SSID, IEEE mode, channel configuration, security, advanced radio settings.

Virtual AP : create and setup virtual AP (only in AP wireless mode).

Wireless ACL : access control by MAC address (only in 570n and IPoll 570n wireless modes).

Traffic shaping : download and upload traffic control.

Port forwarding : port forwarding rules (only in router network mode for AP and IPoll AP).

Static routes : static route rules (only in router network mode for AP and IPoll AP).

Services

WNMS : set WNMS server/collector URL allowing remote device configuration and monitoring.

System alerts : set alerts which can be sent via SNMP Traps or/and SMTP notifications.

SNMP : SNMP service settings allowing remote device monitoring.

Clock/NTP : set device date manually or enable and configure NTP service.

SSH : control SSH connection.

HTTP : control HTTP connection.

System

Administration : change password, reboot, restore factory default settings, backup/restore configuration, troubleshooting file support.

Log : view device log, set system log forwarding settings.

LED : control operation of LEDs.

Firmware upgrade : upgrade device firmware.

Tools

Antenna alignment : measure received signal quality of the wireless link to align antenna in the best direction.

Site Survey : information about other wireless networks in the local area.

Delayed reboot : setup delayed reboot for 570n unit.

Ping : perform ping command.

Traceroute : perform graphical traceroute command.

Spectrum analyzer : check the signal strength on available channels.

Applying and Saving Configuration Changes

There are three general buttons located on the right top corner of the WEB GUI allowing managing device configuration:

Apply : if pressed new configuration settings are applied instantly. It will take few seconds and the device will be running with new settings. It should be noted that pressing Apply button settings are not written to the permanent memory. Therefore, if the device is rebooted it will start with old configuration settings.

Discard : if pressed parameter changes are discarded. It should be noted that if Apply or Save&Apply is pressed it is not possible to discard changes.

Save&Apply : if pressed new configuration settings are applied instantly and written to the permanent memory.

It is not required to press **Apply** or **Save&Apply** in every Web GUI tab. The device remembers all changes made in every tab and after action button is used, all changes will be applied.

Configuration Guide

This document contain product's powerful web management interface configuration description allowing setups ranging from very simple to very complex.

Status

Information

The Information page displays a summary of status information of your device. It shows important information for the 570n operating mode, network settings.

System information : displays general information about the device.

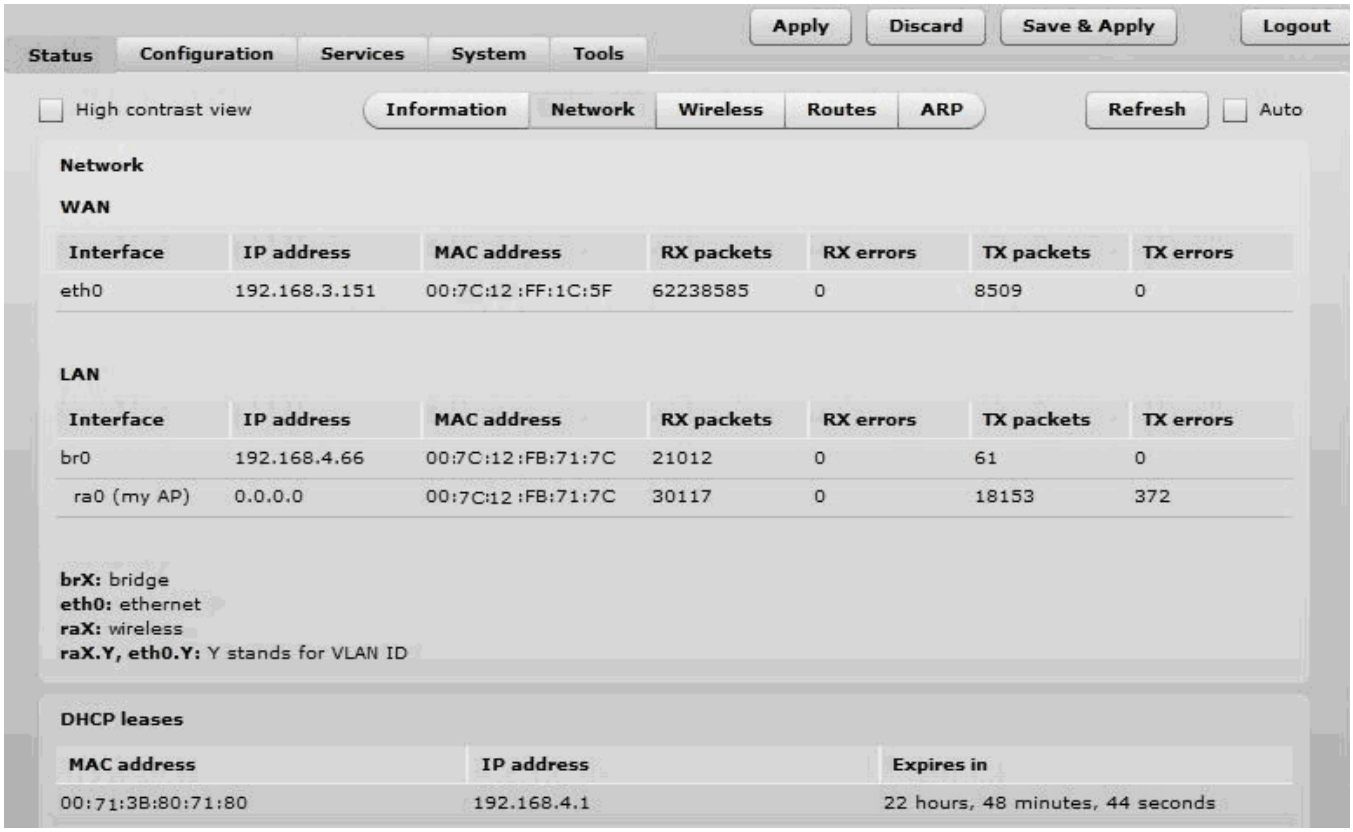
Wireless information : displays general information about the wireless network. The wireless information will differ on Access Point, Station, iPoll wireless modes:

> **AP mode** : displays access point operating information, number of connected clients and SSID details (including APs).
>
> **Station mode** : displays settings at which the station is connected to the access point.
>
> **iPoll AP** : displays iPoll access point operating information, number of connected wireless stations.
>
> **iPoll Station** : displays settings at which the iPoll wireless station is connected to the iPoll access point.

Network mode : displays short summary of the 570n current network configuration (bridge or router).

Network

The Network sections displays statistics of the network interfaces and DHCP leases (depending on network mode: router or bridge):



Interface : displays the interface name. The SSID name is displayed in the brackets near the radio interface (and VAPs).

IP address : displays the IP address of the particular interface.

MAC : displays the MAC address of the particular interface.

Received : displays the number of received packets.

RX errors : displays the number of the RX errors.

Transmitted : displays the number of transmitted packets.

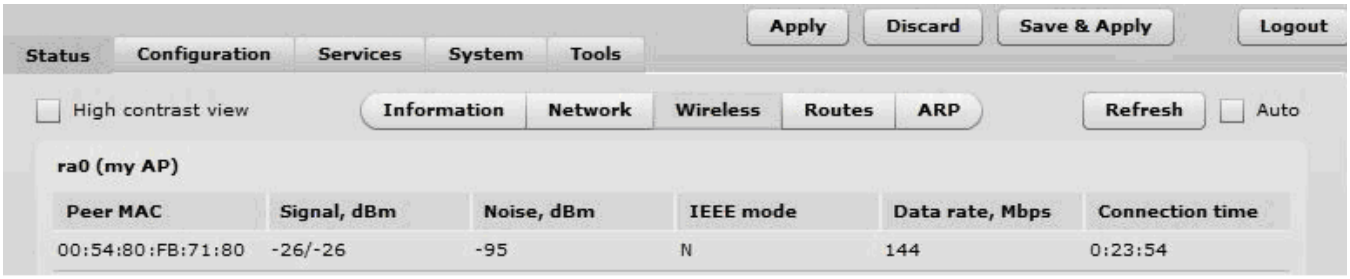
TX errors : displays the number of the TX errors.

DHCP leases : table displays information about leased DHCP addresses.

Wireless

Status / Wireless section is not available if 570n is operating in Station wireless mode. All necessary information about wireless connection with 570n unit is under Information section.

The Wireless statistics displays the receive/transmit statistics of successfully associated wireless clients:



In case the access point has more than one wireless interface (VAPs), the appropriate number of tables with information about connected wireless clients will be displayed.

Peer MAC : displays MAC address of the successfully connected wireless client. **Signal** : indicates the signal strength of the access point main and auxiliary antennas that the station communicates with displayed dBm.

Noise : displays the noise level in dBm.

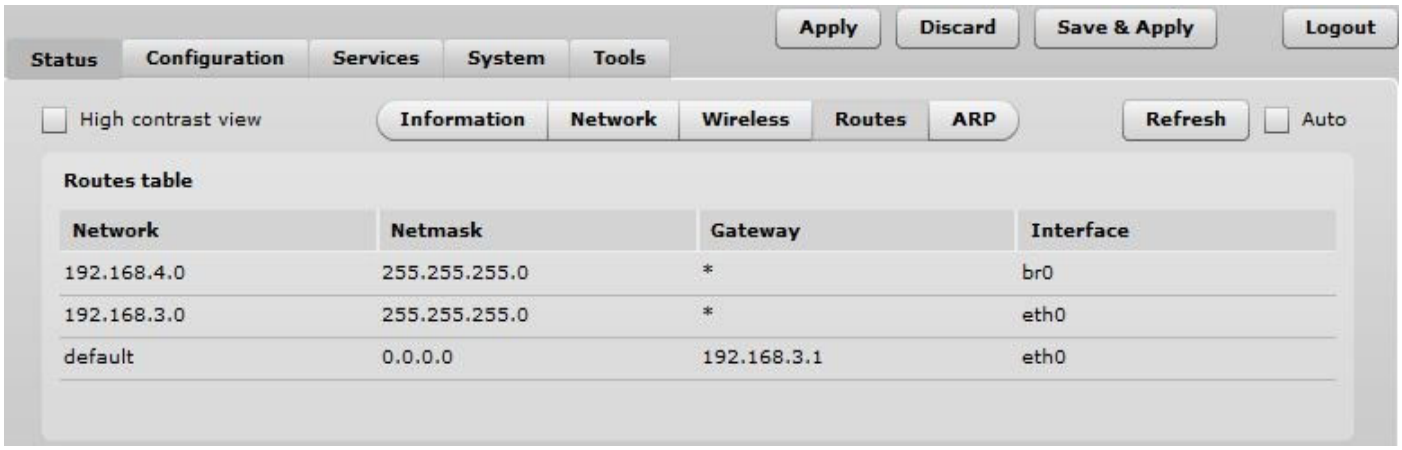
IEEE mode : displays the IEEE mode at which the access point communicates with the particular station.

Data rate : displays the data rate at which the access point communicates with the particular station.

Connection time : displays the duration of the session.

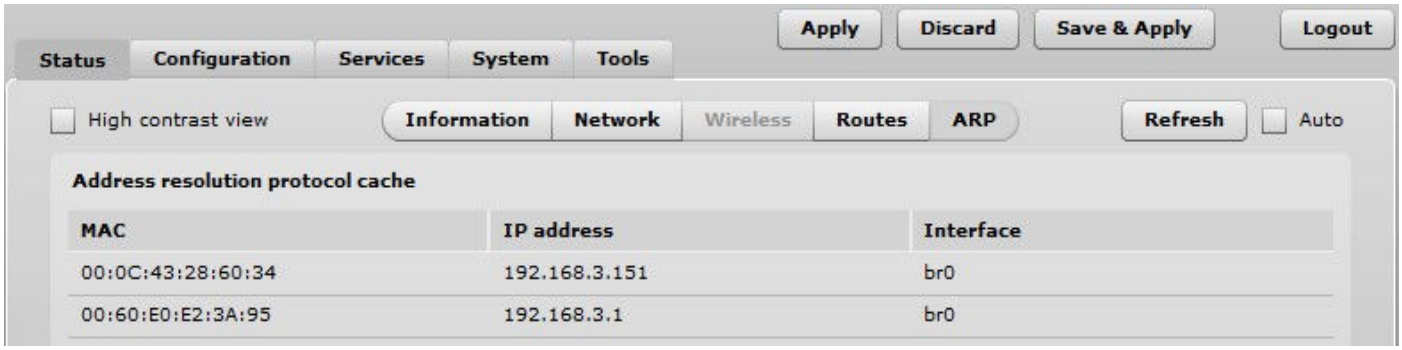
Routes

The Routes page displays the routing table for each interface:



ARP

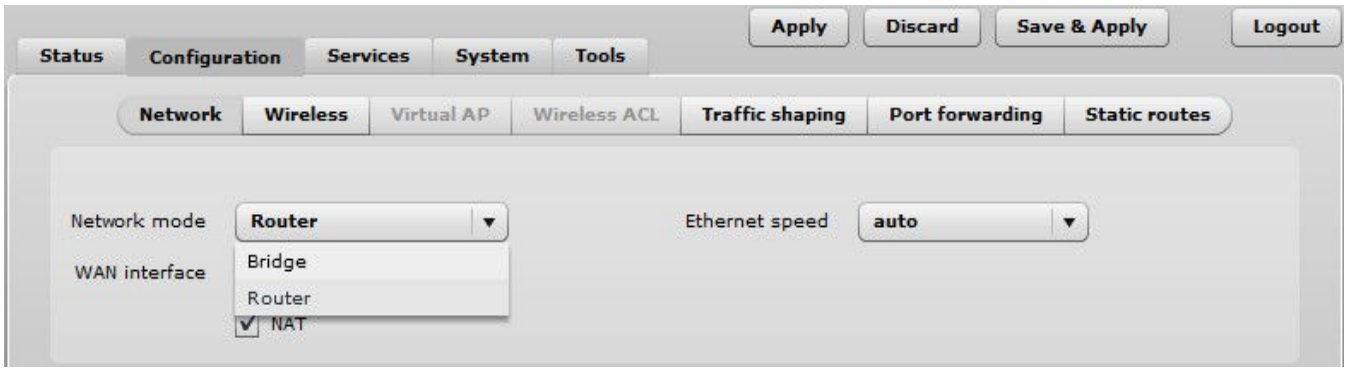
The ARP page displays the ARP (Address Resolution Protocol) table currently recorded on the device. Use Refresh button to reload ARP table results.



Configuration

Network

The **Configuration | Network** page allows you to control the network configuration and settings of the device. First, the device operation mode must be defined to work as a bridge or router. The content of the window varies depending on your selection:



Network mode - choose the device operating mode [bridge/router]

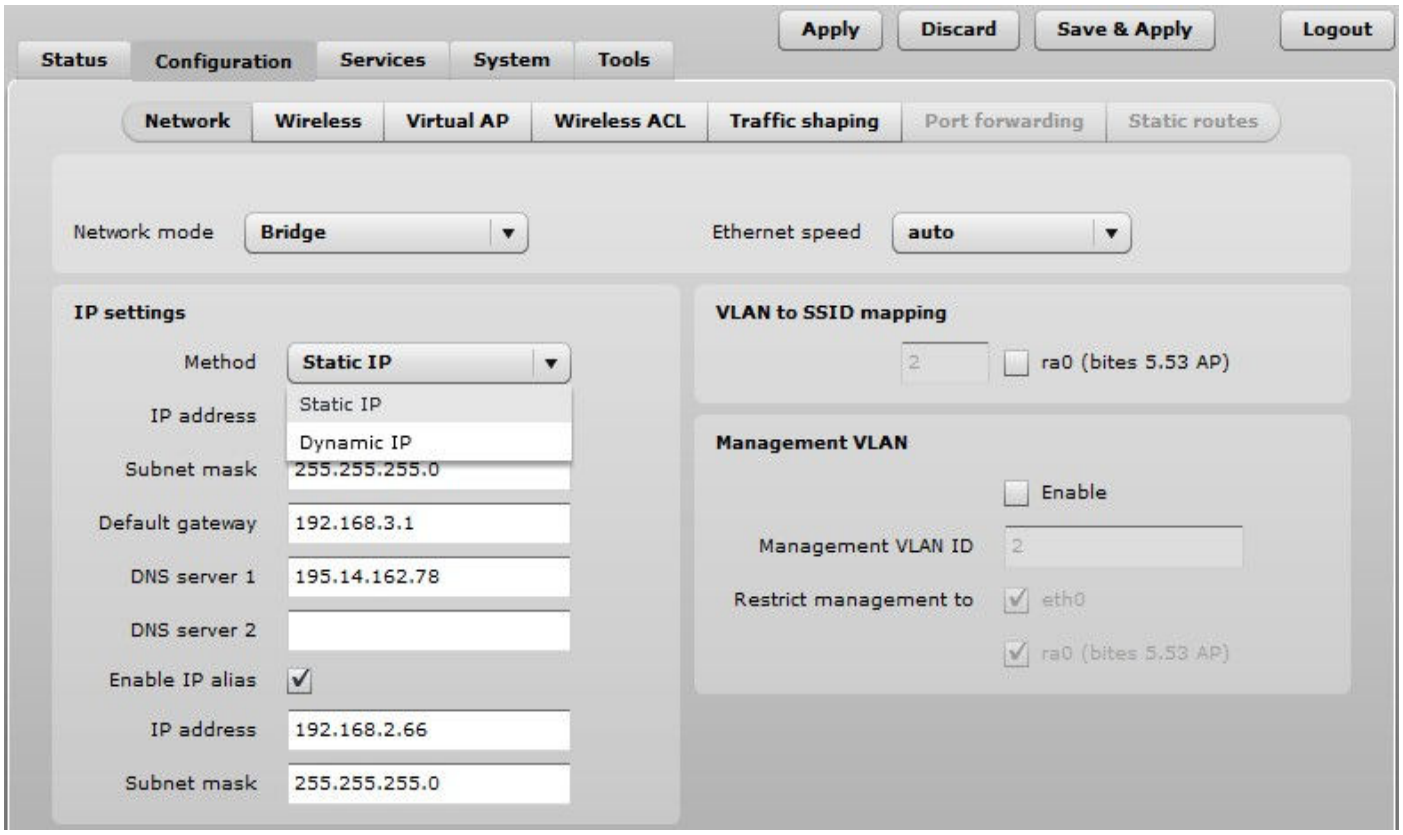
> **Bridge** : in this mode the device works as transparent bridge interconnecting wireless network and LAN port. The Firewall related functions and NAT are not available in this mode.
>
> **Router** : in this mode the device works as router between wireless network and all LAN ports.

Ethernet speed : configures the Ethernet link speed and the duplex mode of the Ethernet port. Choose "auto" for automatic detection of link speed and duplex mode. Network settings will vary according to the selected Network mode. The Bridge mode allows configuring device LAN IP settings, while the Router mode requires more parameters such as LAN network settings, WAN network settings, LAN DHCP settings.

Bridge Mode

Port forwarding and **Static routes** are not available on Bridge mode.

When device is configured to operate in Bridge mode, only device LAN settings should be configured on the **Network** page:



IP Settings

When assigning IP address make sure that the chosen IP address is unused and belongs to the same IP subnet as your wired LAN, otherwise you will lose the connection to the device from your current PC. If you enable the DHCP client, the browser will lose the connection after saving, because the IP address assigned by the DHCP server is not predictable.

Method : specify IP reception method: IP addresses can either be retrieved from a DHCP server or configured manually:

> **Static IP** : the IP address must be specified manually.
>
> **Dynamic IP** : the IP address for this device will be assigned from the DHCP server. If DHCP server is not available, the device will try to get an IP. If has no success, it will use a fallback IP address (default fallback IP is 192.168.2.66). The fallback IP settings can be changed to custom values.

IP Address : specify IP address for device.

Subnet mask : specify a subnet mask for device.

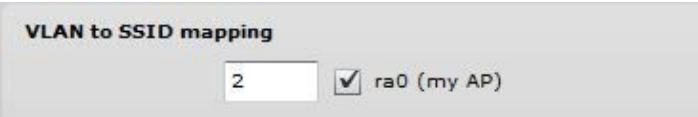
Default gateway : specify a gateway IP address for device.

DNS server : specify the Domain Naming Server.

Enable IP alias : specify the alternative IP address and the netmask for 570n unit management.

VLAN to SSID Mapping

Virtual Local Area Networks (VLANs) are logical groupings of network resources.



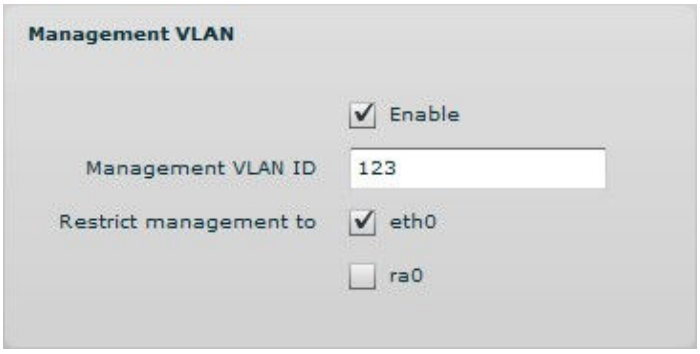
VLAN to SSID mapping : specify the VLAN ID for traffic tagging on required radio interface [2-4095]. The Station devices that associate using the particular SSID will be grouped into this VLAN.

Management VLAN

Available only on Bridge network mode.

Access to the 570n for management purposes can further be limited using VLAN tagging. By defining Management VLAN, the device will only accept management frames that have the appropriate Management VLAN ID. All other frames using any management protocol will be rejected.

When you specify a new management VLAN, your HTTP connection to the device will be lost. For this reason, you should have a connection between your management station and a port in the new management VLAN or connect to the new management VLAN through a multi-VLAN router.



Enable : select to enable a VLAN tagging for management traffic.

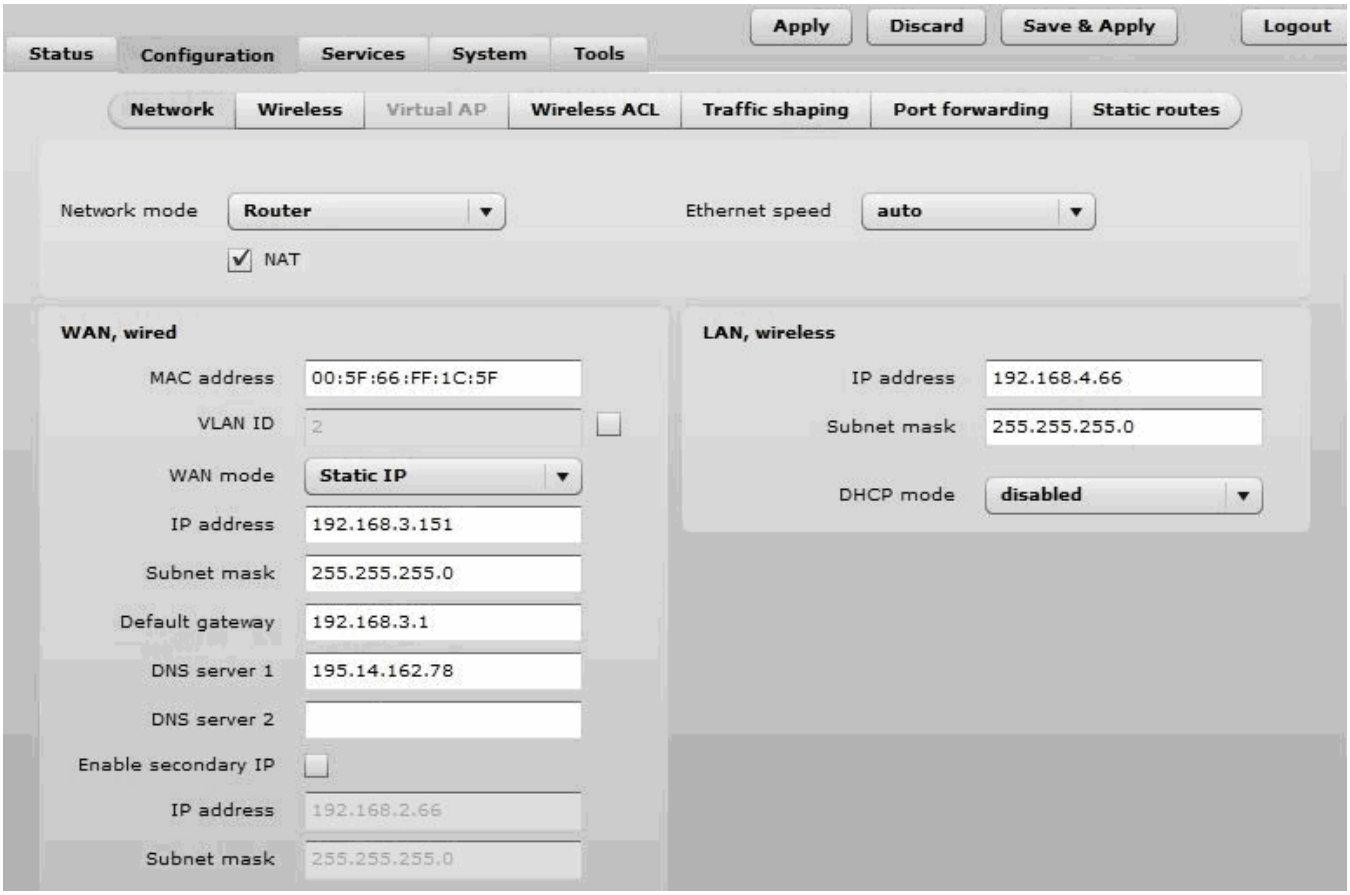
Management VLAN ID : specify the VLAN ID [2-4095]. When device interfaces are configured

with a specific VLAN ID value, only management frames that matching configured VLAN ID will be accepted by device.

Restrict management to interfaces : select interfaces that will be restricted with management VLAN.

Router Mode

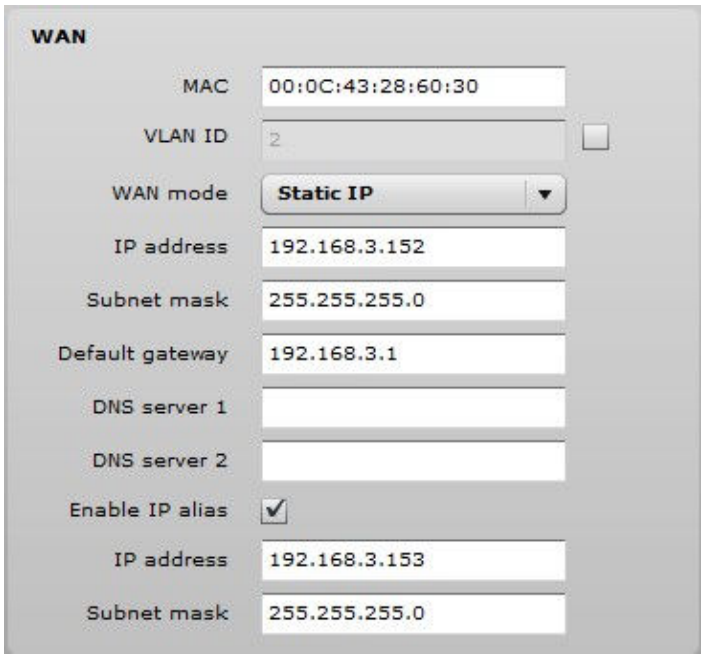
This section allows customizing parameters of the Router to suit the needs of network, including ability to use the built-in DHCP server. When device is configured to operate as Router, the following sections should be specified: WAN network settings, LAN network settings and LAN DHCP settings.



Enable NAT : select to enable NAT (Network Address Translation), that functions by transforming the private IP address of packets originating from hosts on your network so that they appear to be coming from a single public IP address and by restoring the destination public IP address to the appropriate private IP address for packets entering the private network, the multiple PCs on your network would then appear as a single client to the WAN interface.

WAN Settings

WAN network settings include settings related to the WAN interface. The access type of the WAN interface can be configured as: Static IP, Dynamic IP, PPPoE client. **WAN mode** : choose Static IP to specify IP settings for device WAN interface:



MAC address : specify the clone MAC address if required. The ISPs registers the MAC address of the router, and allows only that MAC address to connect to their network. In such case if there is need to change hardware (router), you need to notify your ISP about MAC address change, or simply set the router's MAC address to the MAC address of the previously router/computer.

VLAN ID : specify the VLAN ID for traffic tagging on required radio interface [2-4095]. The

Station devices that associate using the particular SSID will be grouped into this VLAN.

WAN mode : choose Static IP to specify IP settings manually. This option needs parameters

listed below:

IP address : specify static IP address.

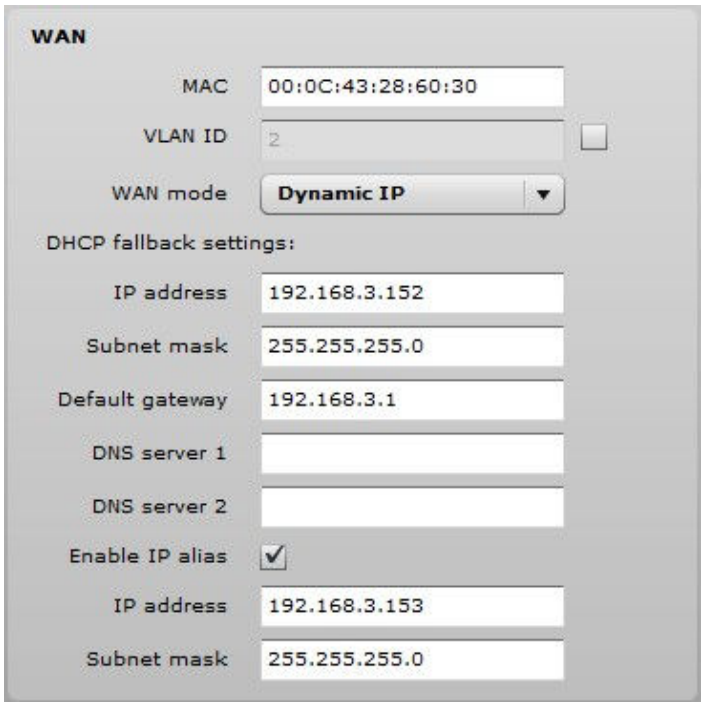
Subnet mask : specify a subnet mask.

Default gateway : specify a gateway.

DNS server : specify primary and/or secondary DNS server

Enable IP alias : specify the alternative IP address and the netmask for 570n unit management.

WAN mode : choose Dynamic IP to enable DHCP client on the WAN side. This option does not need any parameters.



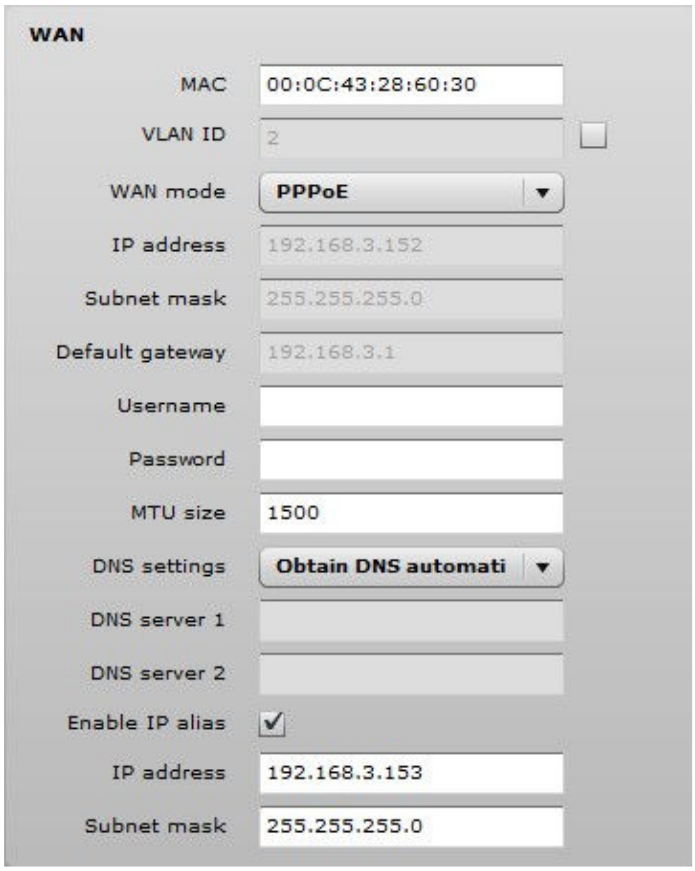
MAC address : specify the clone MAC address if required. The ISPs registers the MAC address of the router, and allows only that MAC address to connect to their network. In such case if there is need to change hardware (router), you need to notify your ISP about MAC address change, or simply set the router's MAC address to the MAC address of the previously router/computer.

VLAN ID : specify the VLAN ID for traffic tagging on required radio interface [2-4095]. The Station devices that associate using the particular SSID will be grouped into this VLAN.

DHCP fallback setting : specify IP address, Subnet mask, Default gateway and optionally DNS server for DHCP fallback. In case the 570n unit will not get the IP address from the DHCP, the specified fallback IP settings will be used.

Enable IP alias : specify the alternative IP address and the netmask for 570n unit management.

WAN mode : choose PPPoE to configure WAN interface to connect to an ISP via a PPPoE:



MAC address : specify the clone MAC address if required. The ISPs registers the MAC address of the router, and allows only that MAC address to connect to their network. In such case if there is need to change hardware (router), you need to notify your ISP about MAC address change, or simply set the router's MAC address to the MAC address of the previously router/computer.

VLAN ID : specify the VLAN ID for traffic tagging on required radio interface [2-4095]. The Station devices

that associate using the particular SSID will be grouped into this VLAN.

User name : specify the user name for PPPoE.

Password : specify the password for PPPoE.

MTU : specify the MTU (Maximum Transmission Unit). The default value is 1500 bytes.

DNS settings : allows selecting if automatically assigned or alternative DNS servers should be used.

Enable IP alias : specify the alternative IP address and the netmask for 570n unit management.

LAN Settings

LAN network settings includes settings related to the LAN interface:

IP address : specify the IP address of the device LAN interface.

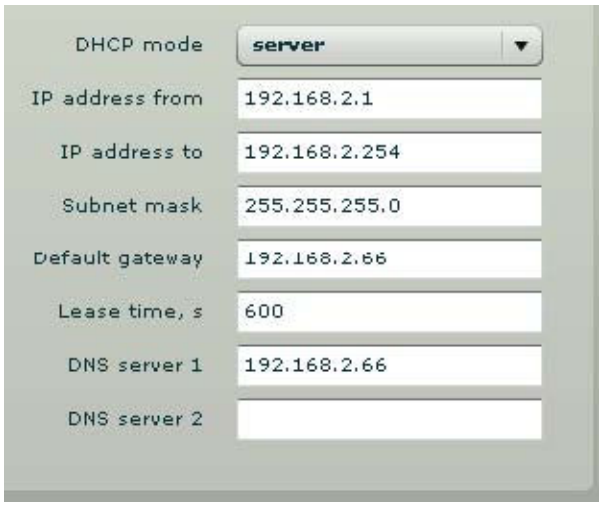
Subnet mask : specify the subnet mask of the device LAN interface.

LAN DHCP Settings

DHCP mode : choose *disabled* to disable DHCP on LAN interface.

DHCP mode : choose *relay* to enable DHCP relay. The DHCP relay forwards DHCP messages between subnets with different sublayer broadcast domains.

DHCP mode : choose *server* to enable DHCP server on LAN interface.



IP address from : specify the starting IP address of the DHCP address pool.

IP address to : specify the ending IP address of DHCP address pool.

Subnet mask : specify the subnet mask.

Default gateway : specify DHCP gateway IP address.

Lease time : specify the expiration time in seconds for the IP address assigned by the DHCP server.

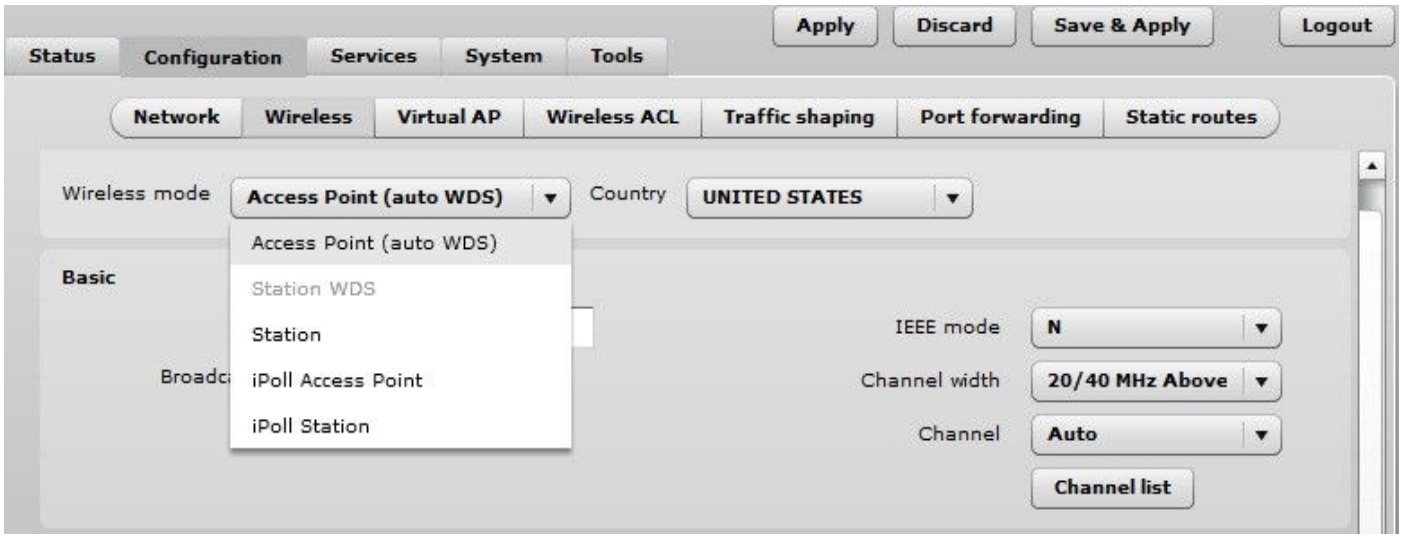
DNS server : specify the DNS server IP address.

Wireless

The Wireless tab is divided in three sections: Basic, Security and Advanced configuration sections. The Basic section contains all parameters that required to configure in order have working wireless link. Security section is used to select authentication and encryption settings. Advanced section contains parameters allowing optimizing the link capacity.

Before changing radio settings manually verify that your settings will comply with local government regulations. At all times, it is the responsibility of the end-user to ensure that the installation complies with local radio regulations.

The 570n can operate in five wireless modes: *Access Point*, *Station*, *Station WDS*, *iPoll Access Point* and *iPoll Station*.



Depending on the wireless operation mode selection some of the displayed configuration parameters will differ (e.g. security or advanced wireless settings).

Wireless mode **: select wireless operation mode:**

Access Point (auto WDS) : enables the 570n radio to function as an access point. When in Access Point mode, wireless clients can see the 570n broadcast and associate to it.

Station : sets the radio to run in client mode. In this mode the 570n does not broadcast an SSID and clients cannot connect to it. Station mode allows the 570n radio to connect to other access points.

Station WDS : a 570n station will communicate with a 570n access point in WDS mode. Station WDS mode enables packet forwarding at layer 2 level.

iPoll Access Point : enables 570n to function as an access point for point-to-multipoint solution. The iPoll Access Point accepts only iPoll Station requests.

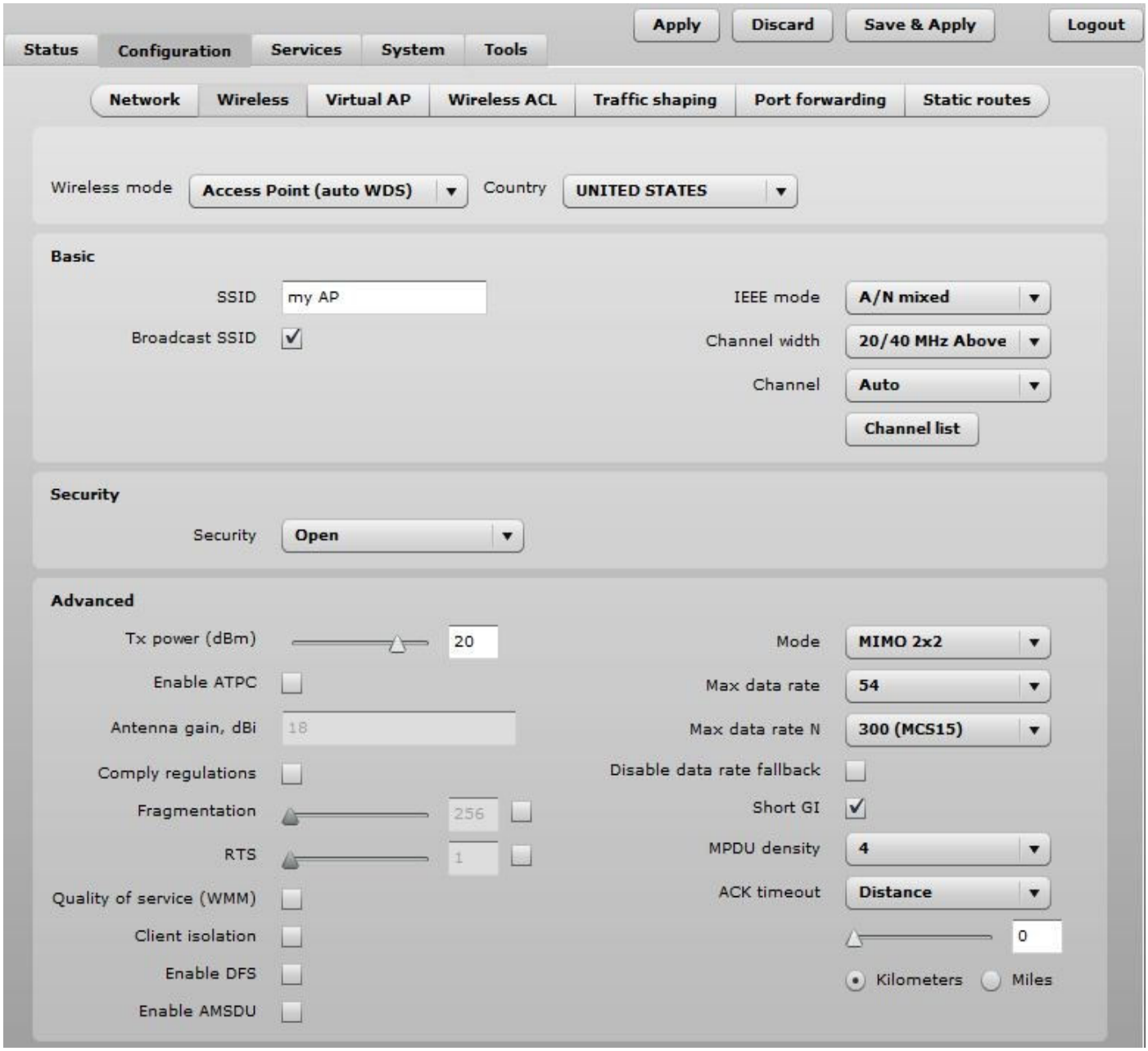
iPoll Station : enables 570n to function as a wireless station for point-to-multipoint solution. The iPoll Station can establish a link only with iPoll Access point.

Be sure that both ends of the link have the appropriate wireless mode, otherwise the connection will be not established (e.g. iPoll Station is able to establish a connection only with iPoll Access Point).

Country : choose from the drop-down list the country in which the 570n will operate. The channel list, transmit power limits, IEEE 802.11 mode will be adjusted according to the regulations of the selected country.

Wireless Mode: Access Point (auto WDS)

Use Basic Wireless Settings to setup radio interface of the device.



570n Basic Wireless Settings

SSID : specifies the SSID of the wireless network device.

Broadcast SSID : enables or disables the broadcasting of the SSID.

IEEE mode : specify the wireless network mode.

Channel width : The default channel bandwidth for 802.11 radio is 20MHz. The 802.11n allow channel bonding in such way the total channel width becomes 40MHz.

Channel : select the channel from the drop-down list or option Auto for auto channel. Automatic channel selection allows Access Point to select a channel which is not used by any other wireless device or, if there are no free channels available - to select a channel which is least occupied.

Channel list : select the channels to create a channel list for autochannel.

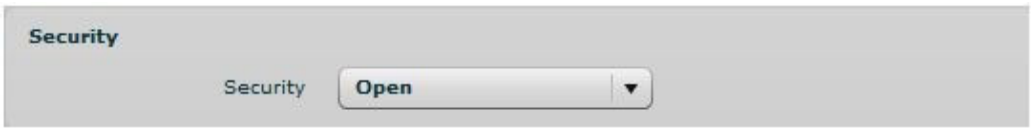
570n Security Settings

Both sides (AP and Station) of the link must have the same security settings.

Device supports various authentication/encryption methods:

Open : no encryption.
WEP : 64bit and 128bit key based encryption.
Personal : preshared key encryption with WPA/WPA2 using AES or TKIP.
Enterprise : RADIUS server based authentication with WPA/WPA2 encryption using AES or TKIP (requires configured RADIUS server).
UAM : Web browser based user authentication method. UAM authentication is available only if Access Point is working in router mode. For UAM configuration details refer at the respective chapter Universal Access Method (UAM).

By default there is no encryption enabled on the device:



WEP encryption can be either 64bit or 128bit:

WEP passkey : specify the passkey, for the chosen WEP security:

For **WEP 64bit** encryption : 5 HEX pairs (e.g. aa:bb:cc:dd:ee), or 5 ASCII characters (e.g. abcde);

For **WEP 128bit** encryption : 13 HEX pairs (e.g. aa:bb:cc:dd:ee:ff:gg:hh:00:11:22:33:44), or 13 ASCII characters (e.g. abcdefghijklm);

To setup **Personal WPA/WPA2** encryption, need to specify the pre-shared key and encryption with chosen AES, TKIP or Auto method:

Passphrase : specify WPA or WPA2 passphrase [8-63 characters]. The passphrase will be converted to key format, selected above.

Encryption : specify WPA/WPA2 encryption algorithm:

> **AES** : 570n will accept clients with passphrase encrypted with AES method only;
> **TKIP** : 570n will accept clients with passphrase encrypted with TKIP method only;
> **Auto** : 570n will accept clients with passphrase encrypted with both: AES and TKIP methods;

570n has possibility to configure **Enterprise WPA/WPA2** encryption with RADIUS authentication. Properly configured 570n will accept wireless stations requests and will send the information to configured RADIUS server for client authentication.

The properly configured RADIUS server is required for **Enterprise WPA/WPA2** encryption.

Encryption : specify WPA/WPA2 encryption algorithm:

> **AES** : 570n will accept clients with passphrase encrypted with AES method;
>
> **TKIP** : 570n will accept clients with passphrase encrypted with TKIP method;
>
> **Auto** : 570n will accept clients with passphrase encrypted with both: AES and TKIP methods;

RADIUS authentication settings:

RADIUS IP : specify the IP address of the authentication RADIUS server where the authentication requests will be send to.

RADIUS port : specify the network port used to communicate with the RADIUS authentication server. Default: 1812 for authentication.

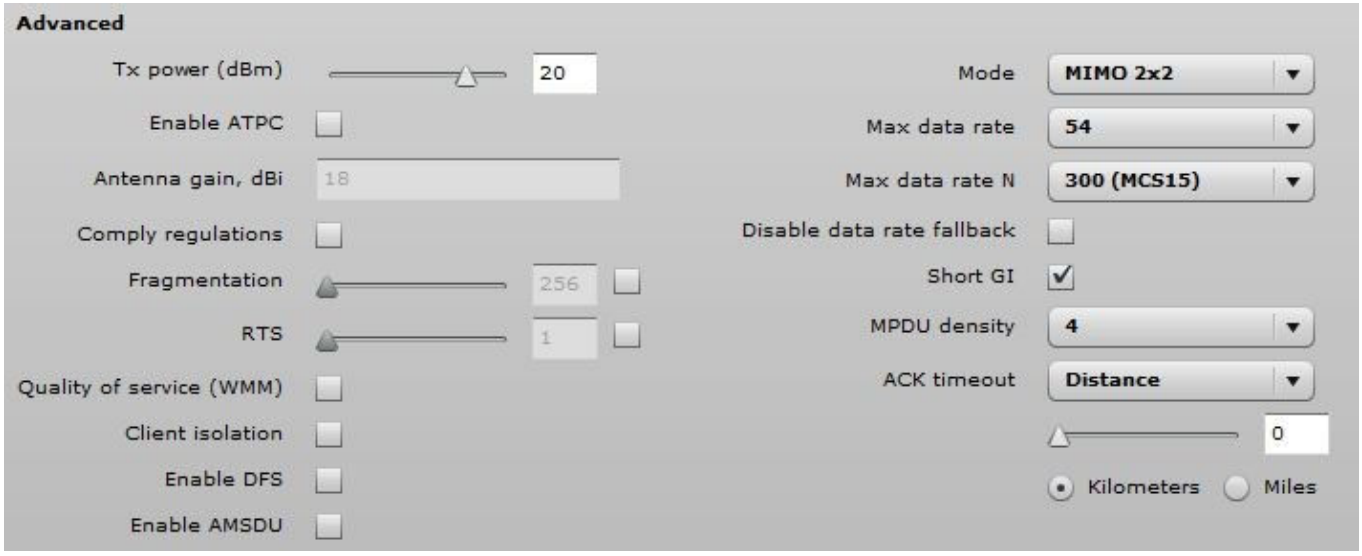
RADIUS key : specify the secret key of the authentication server [string]. The shared secret

is used to encrypt data packets transmitted between RADIUS server and client.

The RADIUS key must be the same on the RADIUS servers and the RADIUS client.

570n Advanced Wireless Settings

Advanced parameters allow configuring the device to get the best performance/capacity of the link.



Tx power : set the unit's transmitting power at which the device will transmit data. The larger the distance, the higher transmit power is required. To set transmit power level use the slider or enter the value manually. When entering the transmit power value manually, the slider position will change according to the entered value. The maximum transmit power level is limited to the allowed value by country in which device is operating regulatory agency.

Enable ATPC : select to enable Automatic Transmit Power Control (ATPC). If enabled, device radio will continuously communicate with remote unit's radio in order to adjust the optimal transmit power automatically.

Antenna Gain, dBi : displays integrated antenna gain in dBi. This entry field will be editable for the connected antennas where the custom value of the antenna gain must be specified.

Comply regulations : if enabled, the 570n will automatically adjust radio settings (transmit power and DFS) to conform regulatory rules of the selected country.

Fragmentation : specify the Fragmentation threshold using slider or enter the value manually [256-2346 bytes]. This is the maximum size for a packet before data is fragmented into multiple packets. Setting the Fragmentation threshold too low may result in poor network performance. Only minor modifications of this value are recommended.

RTS : specify the RTS threshold using slider or enter the value manually [0-2347 bytes]. The RTS threshold determines the packet size of a transmission and, through the use of an access point, helps control traffic flow.

Quality of service (WMM) : enable to support quality of service for traffic prioritizing.

Client isolation : select to enable the layer 2 isolation that blocks clients from communicating with each other. Client isolations is available only in Access Point (auto WDS) mode.

Enable DFS : select to enable radar detection. With enabled DFS, 570n unit monitors the operating frequency for radar signals. If radar signals are detected on the channel, the 570n unit randomly selects a different channel.

Enable AMSDU : enable the AMSDU packet aggregation. If enabled, the maximum size of the 802.11 MAC frames will be increased.

Mode : choose the 570n antenna operating mode:

> **SISO** : single input single output. The device will use 1x1 antenna for data transfer. The antenna will be chosen automatically.
> **MIMO** : multiple input multiple output. The device will use 2x2 antenna for data transfer (two simultaneous streams).

Max data rate : choose the maximum data rate in Mbps at which should transmit packets. The 570n will attempts to transmit data at the highest data rate set. If there will be an interference encountered, the 570n will step down to the highest rate that allows data transmission.

Max data rate N : choose the data rates in Mbps at which should transmit packets for the selected 802.11n mode. The 570n will attempts to transmit data at the highest data rate set. If there will be an interference encountered, the 570n will step down to the highest rate that allows data transmission.

Disable data rate fallback : when this option is selected, the constant Max data rate will be set without a step back to the next highest data rate for 570n data transmission.

Short GI : enable short guard interval. If selected, then 400ns value will be used, else 800ns.

MPDU density : define minimum time between PPDU's.

ACK timeout : specify the ACK timeout using slider or enter the value manually. Ack timeout can be entered by defining the link distance or specifying time value. Too low value of the ACK timeout will give very low throughput. A high value may slow down the link in noisy environment. A low value is far worse than a value slightly too high. ACK Timeout value should be tuned to the optimal value for the maximum link throughput.

Wireless Mode: Station

Station WDS has the same wireless settings.

The Station wireless settings a bit differ from the Access Point's settings: there is possibility to scan SSID of the surrounding 570ns and choose the required one.

Use Wireless Settings to setup radio interface of the device.

Station Basic Wireless Settings

SSID : specify the SSID of the wireless network device.

Scan : click this button to scan for surrounding wireless networks. Found network SSID's will be available in drop down menu.

IEEE mode : specify the wireless network mode.

Channel width - The default channel bandwidth for 802.11 radio is 20MHz. The 802.11n allow channel bonding in such way the total channel width becomes 40MHz.

Station Security Settings

Both sides (AP and Station) of the link must have the same security settings.

Device supports various authentication/encryption methods:

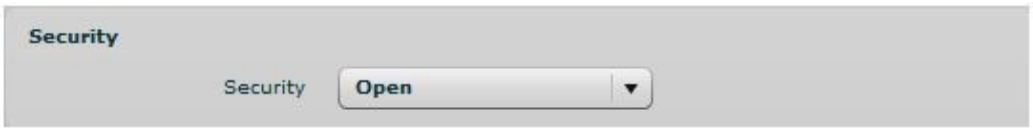
Open : no encryption.

WEP : 64bit and 128bit key based encryption.

Personal : preshared key encryption with WPA/WPA2 using AES or TKIP.

Enterprise : RADIUS server based authentication with WPA/WPA2 encryption using AES or TKIP (requires configured RADIUS server).

By default there is no encryption enabled on the device:



WEP encryption can be either 64bit or 128bit:

WEP passkey : specify the passkey, for the chosen WEP security:

For **WEP 64bit** encryption : 5 HEX pairs (e.g. aa:bb:cc:dd:ee), or 5 ASCII characters (e.g. abcde);

For **WEP 128bit** encryption : 13 HEX pairs (e.g. aa:bb:cc:dd:ee:ff:gg:hh:00:11:22:33:44), or 13 ASCII characters (e.g. abcdefghijklm);

Personal WPA/WPA2 encryption must be specified with the pre-shared key, encrypted with chosen AES or TKIP method (Auto mode on Station is not available):

Passphrase : specify WPA or WPA2 passphrase [8-63 characters]. The passphrase will be converted to key format, selected above.

Encryption : specify WPA/WPA2 encryption algorithm:

AES : passphrase encrypted with AES method;
TKIP : passphrase encrypted with TKIP method only;

Wireless Station has possibility to use **Enterprise WPA/WPA2** encryption with RADIUS authentication. Station will send requests to 570n, which will redirect authentication parameters to required RADIUS server.

Encryption : choose WPA/WPA2 encryption type:

AES : data encrypted with AES method;

TKIP : data encrypted with TKIP method;

Eap method : choose Eap method:

Eap-TTLS-MSCHAPv2

PEap/ MSCHAPv2

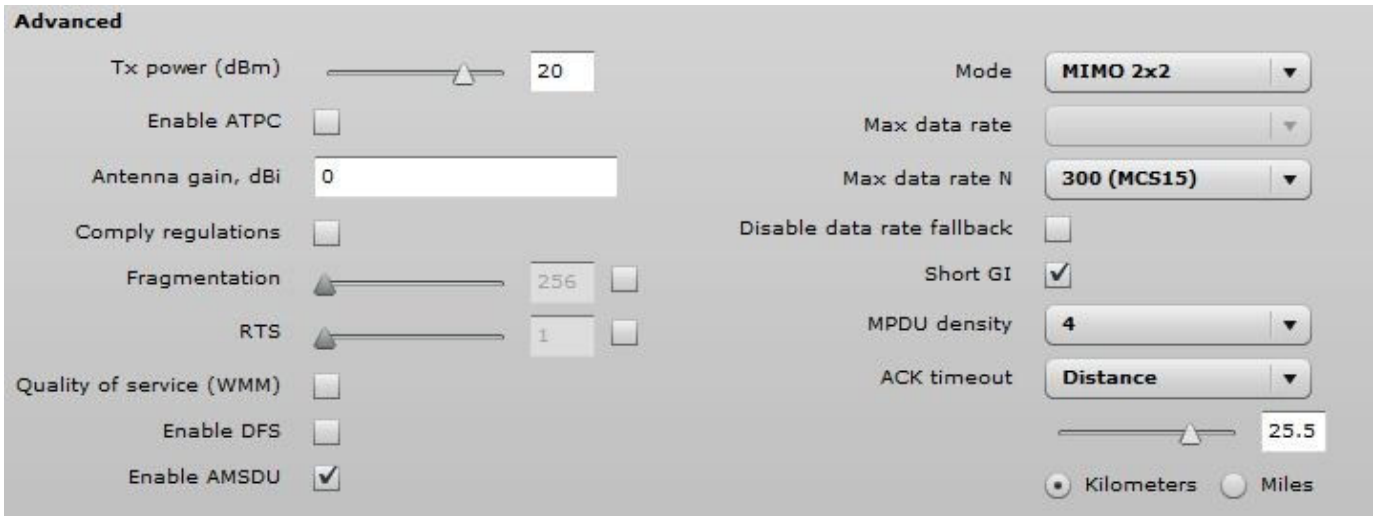
Identity : specify the identity of the authentication to the RADIUS server.

Password : specify the password of the authentication to the RADIUS server.

Identity and Password on the 570n must match the identity and password running on the RADIUS server's user list.

Station Advanced Wireless Settings

Advanced parameters allow configuring the device to get the best performance/capacity of the link.



Tx power : set the unit's transmitting power at which the device will transmit data. The larger the distance, the higher transmit power is required. To set transmit power level use the slider or enter the value manually. When entering the transmit power value manually, the slider position will change according to the entered value. The maximum transmit power level is limited to the allowed value by country in which device is operating regulatory agency.

Enable ATPC : select to enable Automatic Transmit Power Control (ATPC). If enabled, device radio will continuously communicate with remote unit's radio in order to adjust the optimal transmit power automatically.

Antenna Gain, dBi : displays integrated antenna gain in dBi. This entry field will be

editable for the connectorized antennas where the custom value of the antenna gain must be specified.

Comply regulations : if enabled, the 570n will automatically adjust radio settings (transmit power and DFS) to conform regulatory rules of the selected country.

Fragmentation : specify the Fragmentation threshold using slider or enter the value manually [256-2346 bytes]. This is the maximum size for a packet before data is fragmented into multiple packets. Setting the Fragmentation threshold too low may result in poor network performance. Only minor modifications of this value are recommended.

RTS : specify the RTS threshold using slider or enter the value manually [0-2347 bytes]. The RTS threshold determines the packet size of a transmission and, through the use of an access point, helps control traffic flow.

Quality of service (WMM) : enable to support quality of service for traffic prioritizing.

Enable DFS : select to enable radar detection. With enabled DFS, 570n unit monitors the operating frequency for radar signals. If radar signals are detected on the channel, the 570n unit randomly selects a different channel.

Enable AMSDU : enable the AMSDU packet aggregation. If enabled, the maximum size of the 802.11 MAC frames will be increased.

Mode : choose the 570n antenna operating mode:

SISO : single input single output. The device will use 1x1 antenna for data transfer. The antenna will be chosen automatically.

MIMO : multiple input multiple output. The device will use 2x2 antenna for data transfer (two simultaneous streams).

Max data rate : choose the maximum data rate in Mbps at which should transmit packets. The 570n will attempts to transmit data at the highest data rate set. If there will be an interference encountered, the 570n will step down to the highest rate that allows data transmission.

Max data rate N : choose the data rates in Mbps at which should transmit packets for the selected 802.11n mode. The 570n will attempts to transmit data at the highest data rate set. If there will be an interference encountered, the 570n will step down to the highest rate that allows data transmission.

Disable data rate fallback : when this option is selected, the constant Max data rate will be set without a step back to the next highest data rate for 570n data transmission.

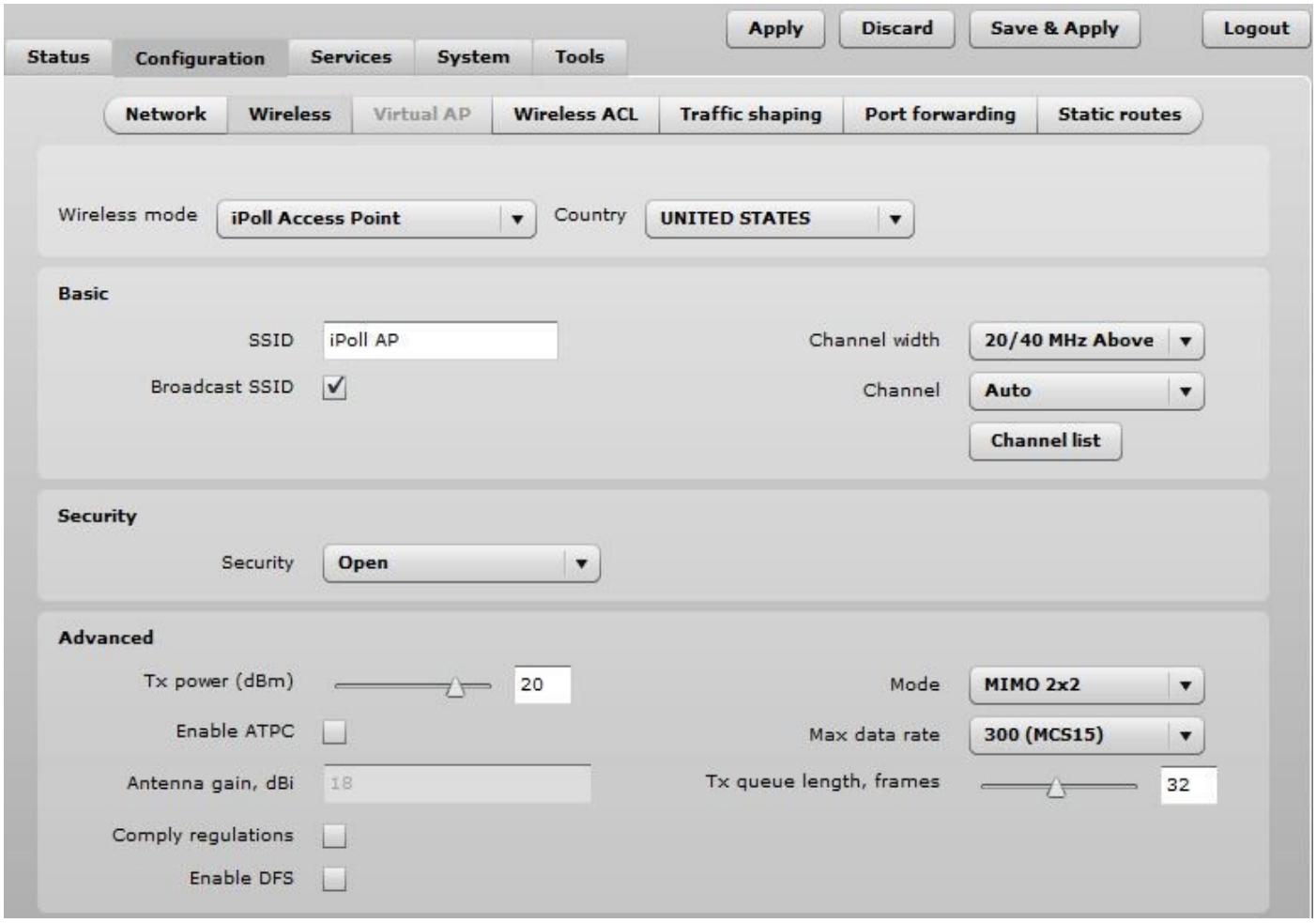
Short GI : enable short guard interval. If selected, then 400ns value will be used, else 800ns.

MPDU density : define minimum time between PPDU's.

ACK timeout : specify the ACK timeout using slider or enter the value manually. Ack timeout can be entered by defining the link distance or specifying time value. Too low value of the ACK timeout will give very low throughput. A high value may slow down the link in noisy environment. A low value is far worse than a value slightly too high. ACK Timeout value should be tuned to the optimal value for the maximum link throughput.

Wireless Mode: iPoll Access Point

The iPoll wireless mode is designed for point to multipoint wireless solutions. The iPoll Access Point establishes a connection only with iPoll Stations thus creating a reliable network.



iPoll 570n Basic Wireless Settings

Use Basic section to setup basic operating settings of the iPoll Access Point's radio.

iPoll Access Point and iPoll Station will operate in 802.11n IEEE mode only.

SSID : specify the SSID of the wireless network device.

Broadcast SSID : enables or disables the broadcasting of the SSID for 570n.

Channel width : The default channel bandwidth for 802.11n radio is 20MHz. The 802.11n allow channel bonding in such way the total channel width becomes 40MHz.

Channel : select the channel from the drop-down list or option Auto for autochannel. Automatic channel selection allows iPoll Access Point to select a channel which is not used by any other wireless device or, if there are no free channels available - to select a channel which is least occupied.

Channel list : select the channels to create a channel list for autochannel.

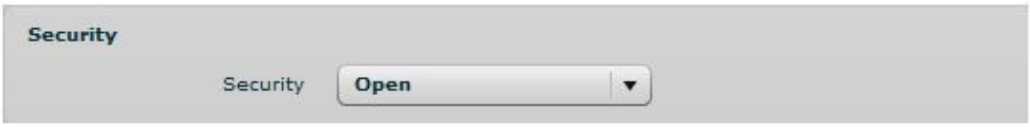
iPoll 570n Security Settings

Both sides (iPoll Access Point and iPoll Station) of the link must have the same security settings.

The 570n device working, in iPoll Access Point wireless mode, supports authentication/encryption methods listed below:

Open : no encryption.
Personal WPA : preshared key encryption with WPA using AES method.
Personal WPA 2 : preshared key encryption with WPA2 using AES method.

By default there is no encryption enabled on the device:



Personal WPA/WPA2 encryption must be specified with the pre-shared key:

Passphrase : specify WPA or WPA2 passphrase [8-63 characters]. The passphrase will be converted to key format, selected above.

iPoll 570n Advanced Wireless Settings

Advanced wireless settings allow configuring the 570n unit to get the best performance/capacity of the link:

Transmit power : set the unit's transmitting power at which the device will transmit data. The larger the distance, the higher transmit power is required. To set transmit power level use the slider or enter the value manually. When entering the transmit power value manually, the slider position will change according to the entered value. The maximum transmit power level is limited to the allowed value by country in which device is operating regulatory agency.

Enable ATPC : select to enable Automatic Transmit Power Control (ATPC). If enabled, device radio will continuously communicate with remote unit's radio in order to adjust the optimal transmit power automatically.

Antenna Gain, dBi : displays integrated antenna gain in dBi. This entry field will be editable for the connectorized antennas where the custom value of the antenna gain must be specified.

Comply regulations : if enabled, the 570n will automatically adjust radio settings (transmit power and DFS) to conform regulatory rules of the selected country.

Enable DFS : select to enable a radar detection. With enabled DFS, 570n unit monitors the operating frequency for radar signals. If radar signals are detected on the channel, the unit randomly selects a different channel.

Mode : choose the unit's antenna operating mode:

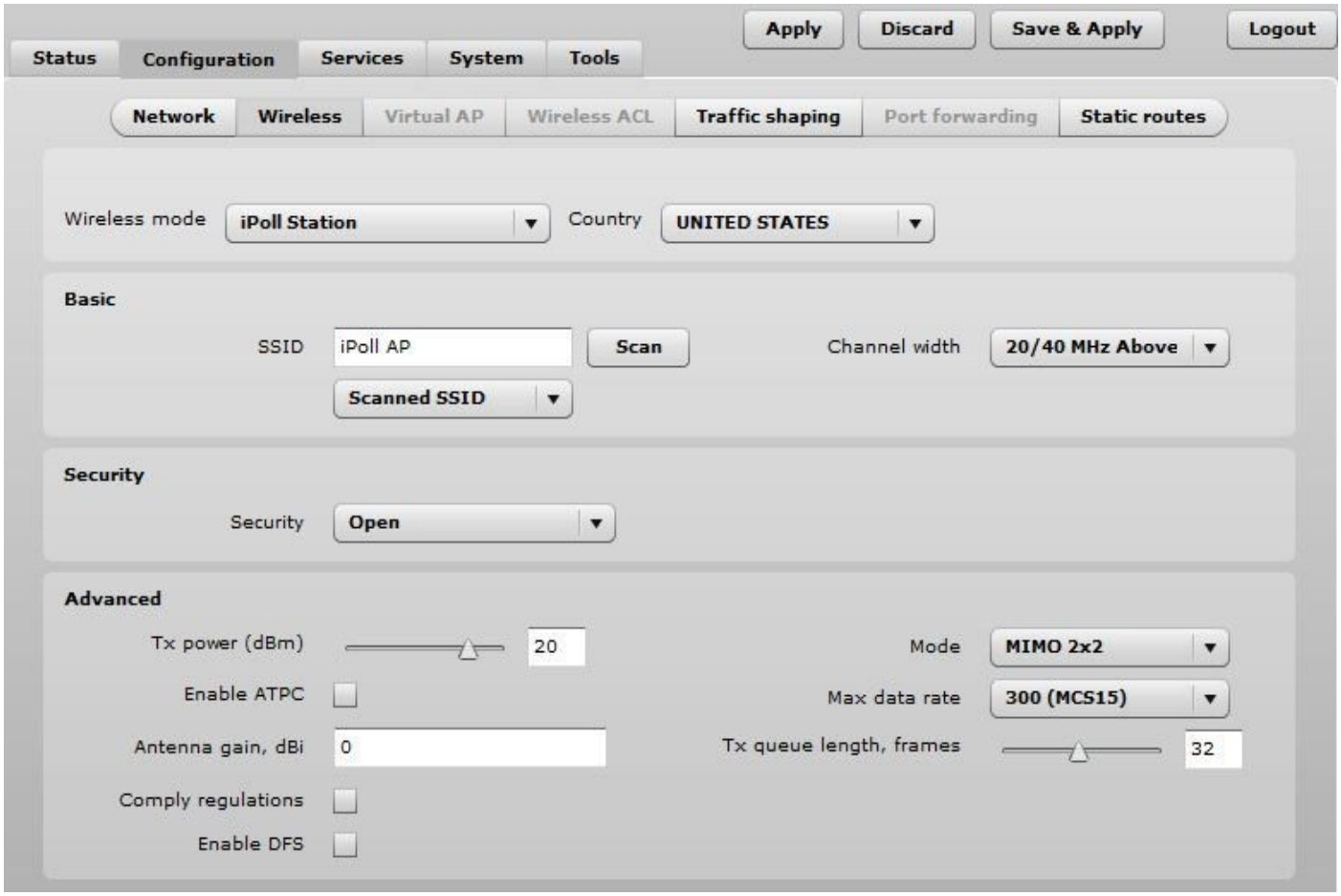
> **SISO** : single input single output. The device will use 1x1 antenna for data transfer. The antenna will be chosen automatically.
> **MIMO** : multiple input multiple output. The device will use 2x2 antenna for data transfer (two simultaneous streams).

Max data rate : select the device data transmission rates in Mbps from the drop-down list. The 570n will attempt to transmit data at the highest data rate set. If there will be an interference encountered, the 570n will step down to the highest rate that allows data transmission.

Transmit queue length, frames : specify the length in frames of the transmit queue.

Wireless Mode: iPoll Station

The iPoll Station is a wireless client mode which can connect to the iPoll Access Points.



iPoll Station Basic Wireless Settings

Use this section to setup basic operating settings of the iPoll Station radio.

iPoll Access Point and iPoll Station will operate in 802.11n IEEE mode only.

SSID : specify the SSID of the wireless network device manually, or use **Scan** to find iPoll access points automatically.

Scan : click this button to scan for surrounding iPoll Access Points. Found network SSID's will be available in drop down menu.

Channel width : The default channel bandwidth for 802.11 N radio is 20/40MHz. The 802.11n allow channel bonding in such way the total channel width becomes 40MHz.

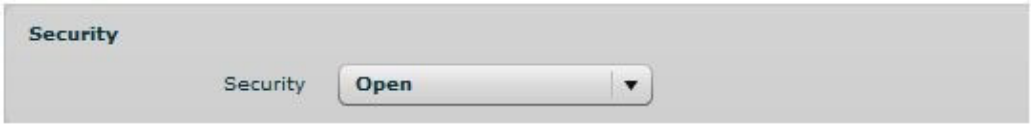
iPoll Station Security Settings

Both sides (iPoll Access Point and iPoll Station) of the link must have the same security settings.

The 570n device working, in iPoll Station wireless mode, supports authentication/encryption methods listed below:

Open : no encryption.
Personal WPA : preshared key encryption with WPA using AES method.
Personal WPA 2 : preshared key encryption with WPA2 using AES method.

By default there is no encryption enabled on the device:



Personal WPA/WPA2 encryption must be specified with the pre-shared key:

Passphrase : specify WPA or WPA2 passphrase [8-63 characters]. The passphrase will be converted to key format, selected above.

iPoll Station Advanced Wireless Settings

Advanced wireless settings allow configuring the 570n unit to get the best performance/capacity of the link:

Transmit power : set the unit's transmitting power at which the device will transmit data. The larger the distance, the higher transmit power is required. To set transmit power level use the slider or enter the value manually. When entering the transmit power value manually, the slider position will change according to the entered value. The maximum transmit power level is limited

to the allowed value by country in which device is operating regulatory agency.

Enable ATPC : select to enable Automatic Transmit Power Control (ATPC). If enabled, device radio will continuously communicate with remote unit's radio in order to adjust the optimal transmit power automatically.

Antenna Gain, dBi : displays integrated antenna gain in dBi. This entry field will be editable for the connectorized antennas where the custom value of the antenna gain must be specified.

Comply regulations : if enabled, the 570n will automatically adjust radio settings (transmit power and DFS) to conform regulatory rules of the selected country.

Enable DFS : select to enable a radar detection. With enabled DFS, 570n unit monitors the operating frequency for radar signals. If radar signals are detected on the channel, the unit randomly selects a different channel.

Mode : choose the unit's antenna operating mode:

> **SISO** : single input single output. The device will use 1x1 antenna for data transfer. The antenna will be chosen automatically.
> **MIMO** : multiple input multiple output. The device will use 2x2 antenna for data transfer (two simultaneous streams).

Max data rate : select the device data transmission rates in Mbps from the drop-down list. The 570n will attempt to transmit data at the highest data rate set. If there will be an interference encountered, the 570n will step down to the highest rate that allows data transmission.

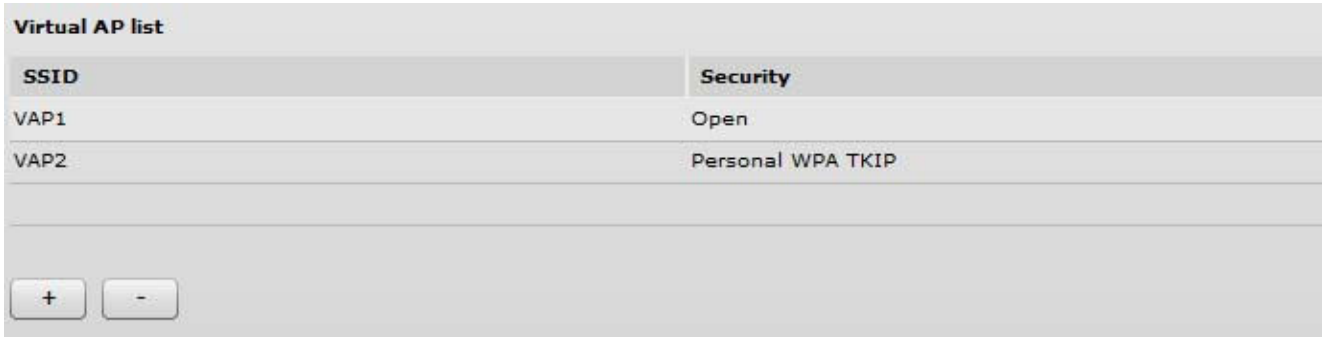
Transmit queue length, frames : specify the length in frames of the transmit queue.

Virtual AP

Virtual AP functionality is available only in **Access Point (auto WDS)** wireless mode.

Use the **Configuration | Virtual AP page** to configure to create up to 3 additional Virtual AP interfaces. The Virtual AP defines a logical wireless network, and the 570n can be configured to provide additional 3 wireless networks on each device radio. All the Virtual APs may be active at the same time meaning that client devices can associate to the 570n using any of the Virtual SSIDs.

The Virtual AP table displays a summary of all virtual radio interfaces running on the 570n:



To create a new Virtual AP, click on **+** button to add new entry on the VAP table, then select this entry and specify required parameters:

SSID : specify the unique name for the VAP [string].

Broadcast SSID : when this option is selected the particular SSID is visible during network scans on a wireless station. When unselected, the VAP SSID is not visible and not broadcasted to wireless stations.

Quality of service (WMM) **: enable to support quality of service for prioritizing traffic.**

User isolation : enable the user Layer 2 isolation. The Layer 2 isolation blocks the wireless clients from communicating with each other.

Each VAP security is configured by default as an "open system", which broadcasts a beacon signal including the configured SSID. For more secure network choose one of the security mechanisms for each VAP interface.

Security : choose the wireless security and encryption method from the drop-down list (for detailed security configuration, refer to the respective section Access Point (auto WDS) Security Settings).

Open : no encryption.
WEP : 64bit and 128bit key.
Personal : preshared key encryption with WPA/WPA2 using AES or TKIP.
Enterprise : RADIUS server based authentication with WPA/WPA2 encryption using AES or TKIP(requires configured RADIUS server).
UAM : Web browser based user authentication method. UAM authentication is available only if Access Point is working in router mode. For UAM configuration details refer at the respective chapter Universal Access Method (UAM).

Wireless clients must be able to respond with a specific security configuration.

Wireless ACL

Wireless ACL is active only in **Access Point (auto WDS)** and iPoll Access Point wireless mode.

Access Control provides the ability to limit associations wirelessly based on MAC address to an 570n by creating an Access Control List (ACL).

Policy : define the policy:

Open : no rules applied

Allow MAC in the list : only listed MAC clients can connect to the 570n (white list).

Deny MAC in the list : only listed MAC clients can NOT connect to the 570n (black list).

To add new rule, press the **"+"** button.

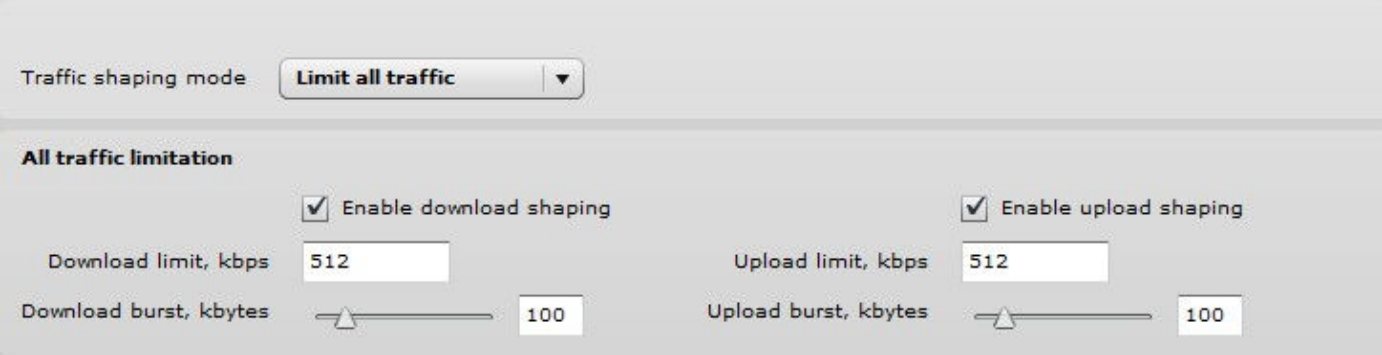
To remove the rule, first select the rule then press the **"?"** button.

To edit the rule double click on the field.

Traffic Shaping

Use Traffic Shaping to control download or upload bandwidth in order to optimize or guarantee performance. There are two methods to control network traffic:

Limit all traffic : limits overall 570n upload and download traffic.
Limit per IP traffic : limits upload and download traffic for a specified IP addresses.



Limit all traffic

Enable download shaping : select to enable limitation of the download traffic.

Download limit, kbps : specify the maximum download (from wireless interface to Ethernet interface) bandwidth value in Kbps.

Download burst, kbytes : specify the download burst size in kbytes.

Enable upload shaping : select to enable limitation of the upload traffic.

Upload limit, kbps : specify the maximum upload (from Ethernet interface to wireless interface) bandwidth value in Kbps.

Upload burst, kbytes : specify the upload burst size in kbytes

Limit per IP traffic

Use **+** button to create new traffic limitation rules:

IP address : specify IP address for which the traffic will be limited.

Down rate, kbps : specify the maximum download (from wireless interface to Ethernet interface) bandwidth value in Kbps.

Down burst, kbytes : specify the download burst size in kbytes.

UP rate, kbps : specify the maximum upload (from Ethernet interface to wireless interface) bandwidth value in Kbps.

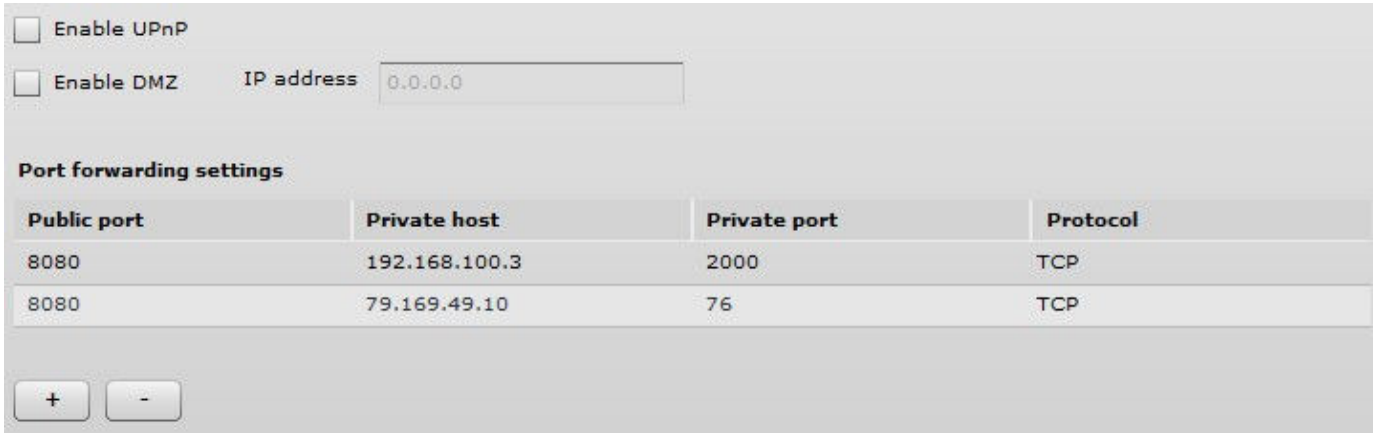
UP burst, kbytes : specify the download burst size in kbytes

Port Forwarding

Port forwarding is active only in Router network mode.

Port Forwarding, **UPnP** and **DMZ** is effective only if NAT is enabled.

The **Port forwarding** section gives the ability to pass traffic behind an interface that has NAT enabled. For instance if the unit is in router mode with NAT enabled on the WAN interface, no devices on the outside of the WAN interface can see any private IPs on the LAN side of the unit. By using port forwarding or DMZ it is possible to pass traffic through to these private IP addresses.



Enable UPnP : select to enable UPnP (Universal Plug and Play connectivity) service. The UPnP enables the 570n to communicate with other network devices automatically opening required ports, without manual intervention.

Enable DMZ : select to enable DMZ. DMZ opens all TCP/UDP ports to particular IP address. It allows setting up servers behind the 570n. The feature is used commonly for setting up VoIP or

Multi-Media servers.

Public port : specify the port that will be accessed externally using the public IP address.

Private host : specify the IP address behind NAT that public traffic will get forwarded to.

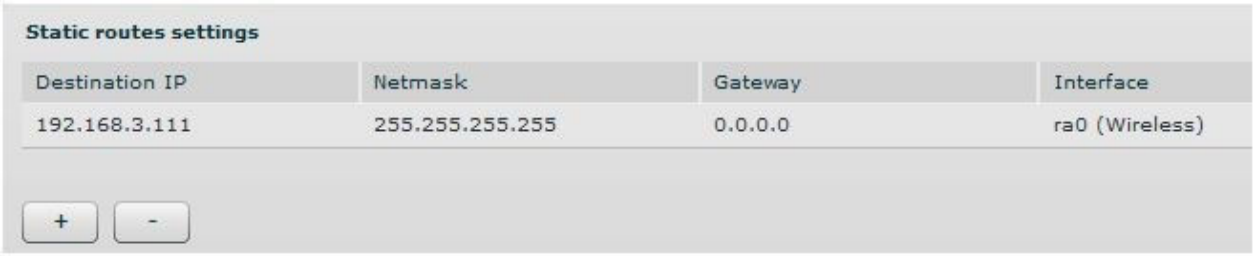
Private port : specify the listening port on private computer behind NAT.

Protocol : select type of forwarding traffic: TCP or UDP.

Static Routes

Static routes is active only in Router network mode.

A routing rule is defined by the destination subnet (Destination IP address and netmask), interface and/or gateway where to route the target traffic. A data packet that is directed to the destination network is routed to the specified router's interface or to another gateway router. To add a new static route, click **+** button and specify the following parameters:



Destination IP : specify the destination IP address.

Netmask : specify destination netmask.

Gateway : specify the gateway address for the route. 0.0.0.0 stands for the default gateway of the selected interface.

Interface : select interface for the route.

Services

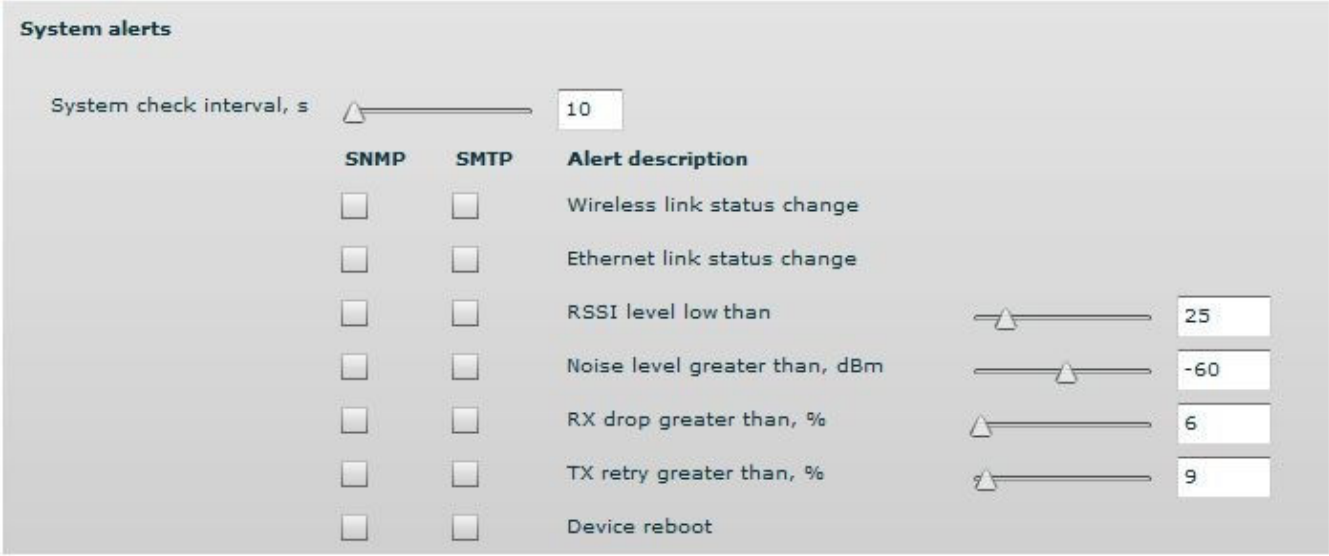
WNMS

Wireless Network Management System (WNMS) is a centralized monitoring and management system for wireless network devices. The communication between managed devices and the WNMS server is always initiated by an WNMS client service running on every device.

Enable WNMS agent : select to enable WNMS agent.
Server/Collector URL : specify the URL of the WMS server to which that heartbeat notifications will be sent to.

System alerts

The device is able to send external alerts when there are system errors. The alerts can be sent via SNMP Traps or/and SMTP notifications.



Enable alerts : select to enable alert notifications on the system.

System check interval, s : specify interval in seconds at which the device will send notifications of unexpected system behavior.

System alerts:

Wireless link status change : system will send notification on Wireless link status change.

Ethernet link status change : system will send notification on Ethernet link status change.

RSSI level lower than : system will send notification when RSSI reach value lower than

specified. Default: 25

Noise level greater than : system will send notification when signal noise will reach value greater than specified. Default: -60 dBm.

RX drop greater than : system will send notification when percent of RX dropped packets become higher than specified value. Default: 250 packets per seconds.

TX retry greater than : system will send notification when percent of TX retries becomes higher than specified value. Default: 250 packets per seconds.

Device reboot : system will send notification about unexpected or administrator initiated device reboot.

SNMP Traps Settings

Manager address : specify the IP address or hostname of SNMP Trap receiver.

Manager port : specify the port number of the Trap receiver. Default port number is 162.

Trap community - specify the SNMP community string. This community string acts as password between SNMP manager and device by default Trap community string is "public".

Use inform : select to wait for an acknowledgment from SNMP manager that Trap was received.

Retry count : specifies maximum number of times to resend an inform request [1-10]. Default: 5.

Retry timeout : specifies number in seconds to wait for an acknowledgment before resending request [1-10]. Default: 1.

SMTP Settings

Server address : specify the IP address or hostname of the networked SMTP server.

Server port : specify the SMTP Port Number is the port number used by the networked SMTP server. By default the port number is 25.

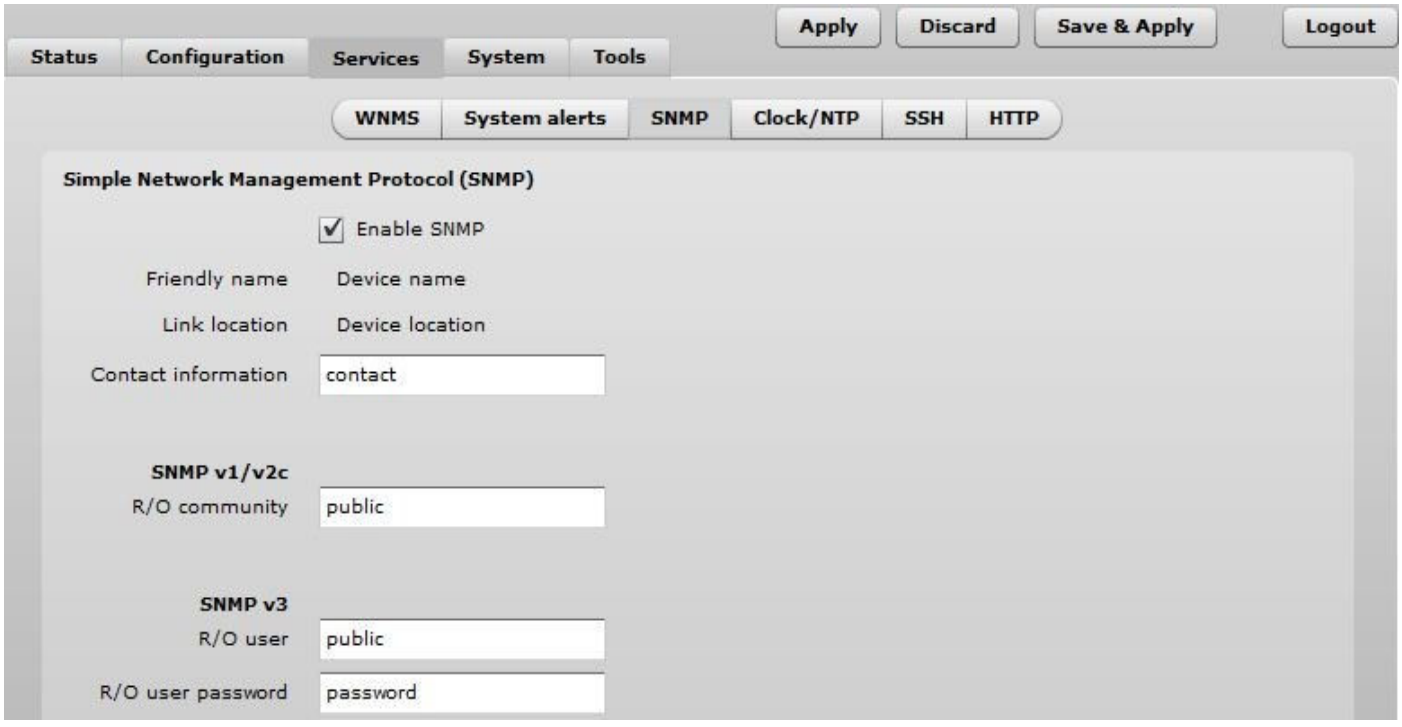
Source e-mail address : specify the e-mail address that will be used by the device.

Destination e-mail address : specify the e-mail address where the device will send the alert messages.

E-mail notification interval : specify interval in seconds at which the e-mail notification will be sent from the device [0-86400]. If 0 specified, then device will send an e-mail notification immediately after unexpected system behavior.

SNMP Settings

SNMP is the standard protocol that is widely used for remote network management over the Internet. With the SNMP service enabled, the device will act as SNMP agent.



Enable SNMP : specify the SNMP service status.

Friendly name : displays name of the 570n that will be used to identify the unit. This name has the same value as Friendly name in the Device settings.

Link location : displays the physical location of the device. This name has the same value as Device location in the Device settings.

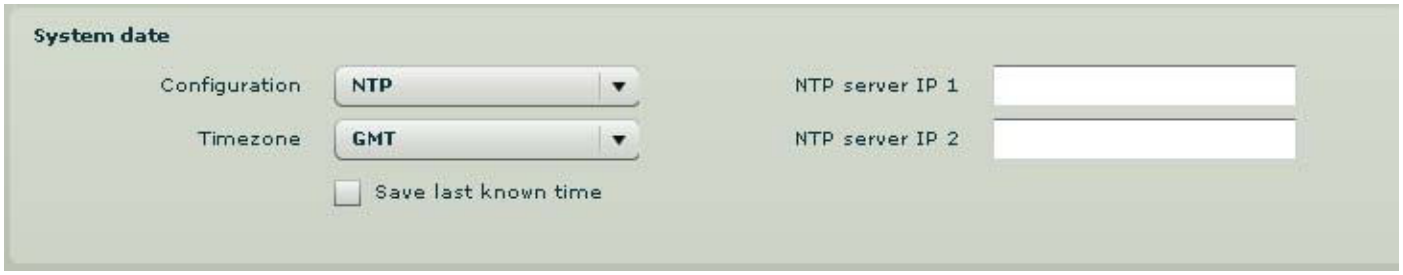
Contact information : specify the identification of the contact person for this managed device, together with information on how to contact this person.
R/O community : specify the read-only community name for SNMP version 1 and version 2c. The read-only community allows a manager to read values, but denies any attempt to change values.

R/O user : specify the user name for read-only SNMPv3 access. The read-only community allows a manager to read values, but denies any attempt to change values.
R/O user password : specify the password for read-only SNMPv3 access [string].

Clock/NTP

Use this section to manage the system time and date on the device automatically, using the Network Time Protocol (NTP), or manually, by setting the time and date on the device.

The NTP (Network Time Protocol) client synchronizes the clock of the device with the defined time server. Choose NTP from the configuration menu, select your location time zone and enter NTP server in order to use the NTP service.



Configuration : choose the system clock configuration mode [NTP/Manual].

Timezone : select the timezone. Time zone should be specified as a difference between local time and GMT time. Save last known time : select to recall the timestamp that was saved on last reboot. When NTP is enabled, this option will set system clock to last reboot time if no NTP servers are available.

NTP server : specify the trusted NTP server IP or hostname for synchronizing time with [IP address].

To adjust the clock settings manually, choose the configuration mode as Manual and specify the following settings:

Configuration : choose the system clock configuration mode [NTP/Manual].

Timezone : select the timezone. Time zone should be specified as a difference between local time and GMT time.

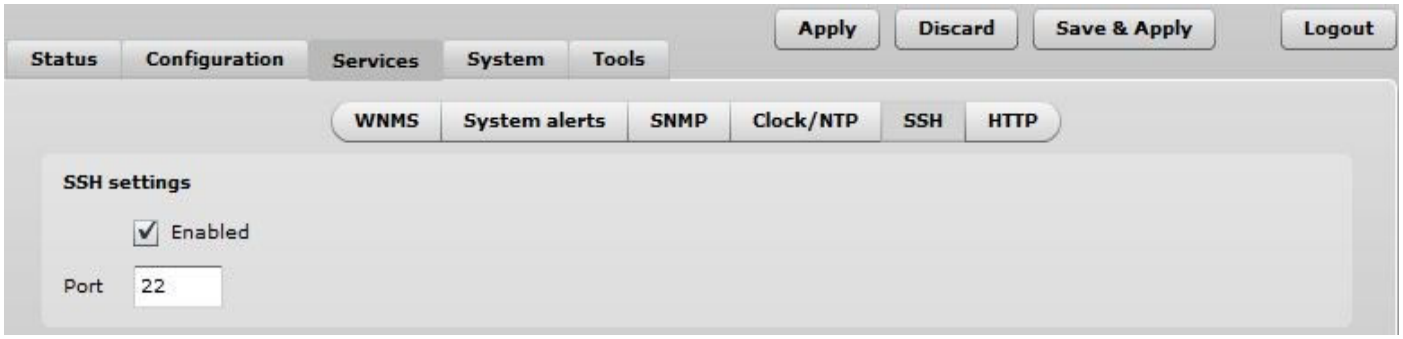
Save last known time : select to recall the timestamp that was saved on last reboot.

Date : specify the new date value in format MM/DD/YYYY

Time : specify the time in format hh:mm.

SSH

Use this menu to manage access to the device via SSH port:

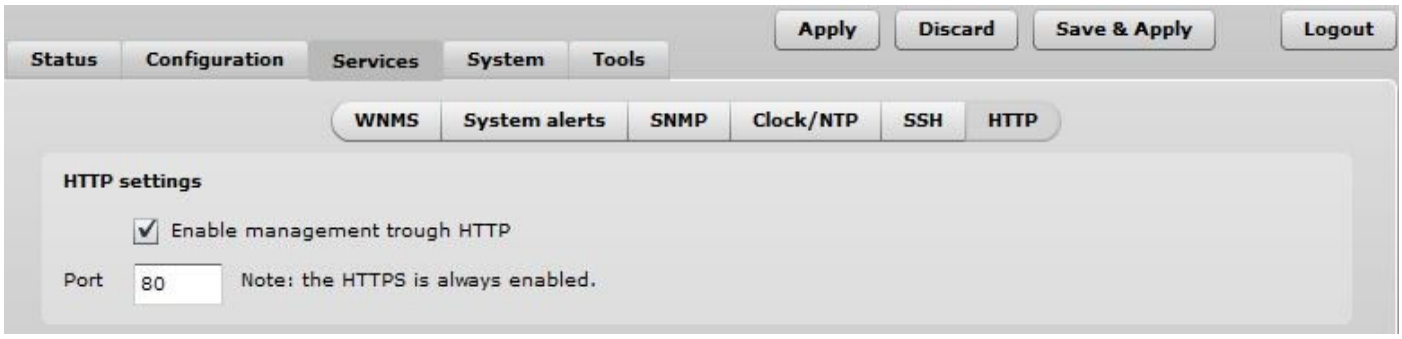


Enabled : enable or disable SSH access to device.

Port : the SSH service port. By default SSH port is 22.

HTTP

Use this menu to control HTTP connection on device web management:



Enable management through HTTP : select tis option to enable or disable HTTP access to the device management.

Port : specify HTTP port. Standard HTTP port is 80.

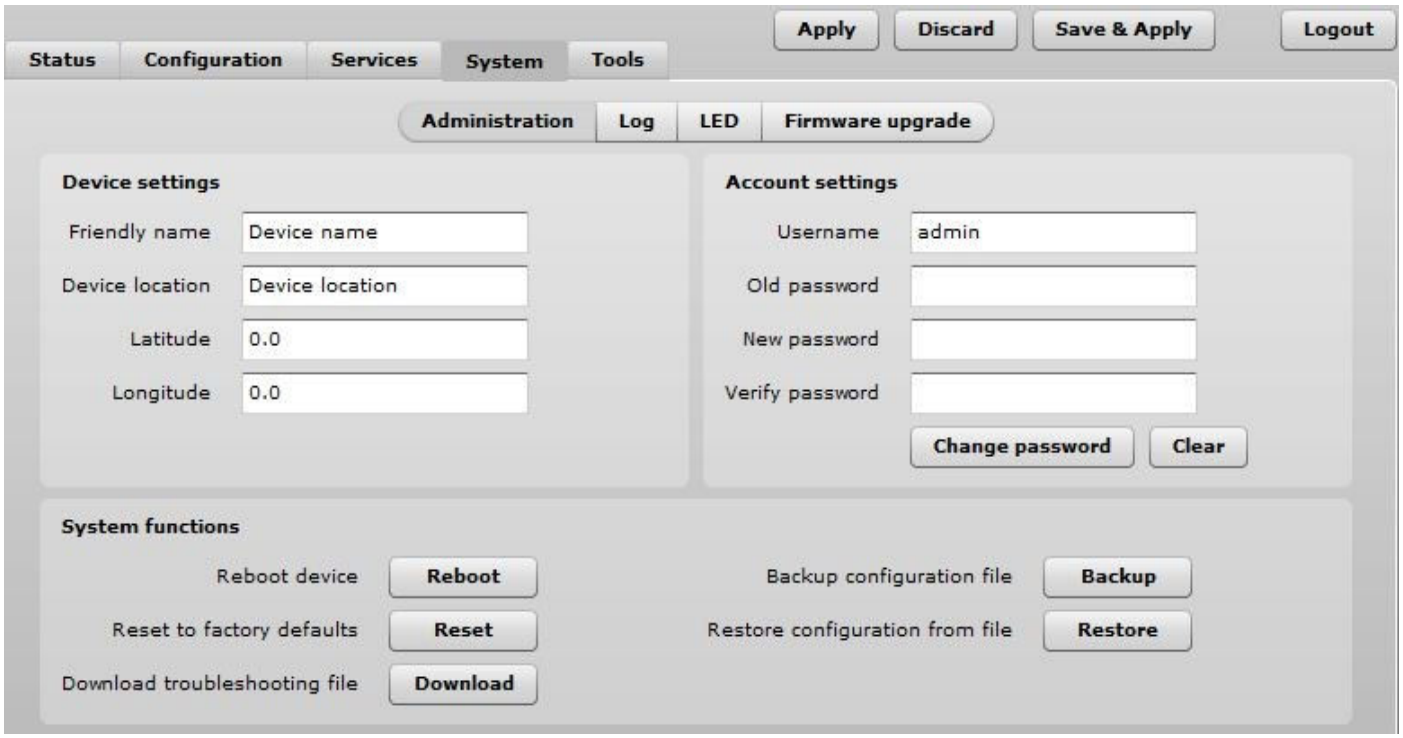
HTTPS connection via the standard port 8080 is always enabled.

System

Administration

For security reasons it is recommended to change the default administrator username and password as soon as possible.

System menu allows you to manage main system settings and perform main system actions (reboot, restore configuration, etc.). The section is divided into further three sections: Device settings, Account settings and system functions.



Device settings

Friendly name : specify name of the 570n that will be used to identify the unit.

Device location : describe the location of the device [maximum 255 ASCII characters].

Longitude : specify the longitude coordinates of the device [specific decimal format, e.q. 54.869446].

Latitude : specify the latitude coordinates of the device [specific decimal format, e.q. 23.891058].

Both coordinates helps indicate accurate location of the device.

Account settings

The Administrative Account menu is for changing the administrator's password.

Default administrator logon settings are:

Username: admin

Password: admin01

Username : change the administrator's username.

Old password : enter the old administrator password.

New password : enter the new administrator password for user authentication.

Verify password : re-enter the new password to verify its accuracy.

The only way to gain access to the web management if you forget the administrator password is to reset the unit to factory default settings.

System functions

Reboot device : reboot device with the last saved configuration.

Reset device to factory defaults : click to restore unit's factory configuration.

Resetting the device is an irreversible process. Current configuration and the administrator password will be set back to the factory default.

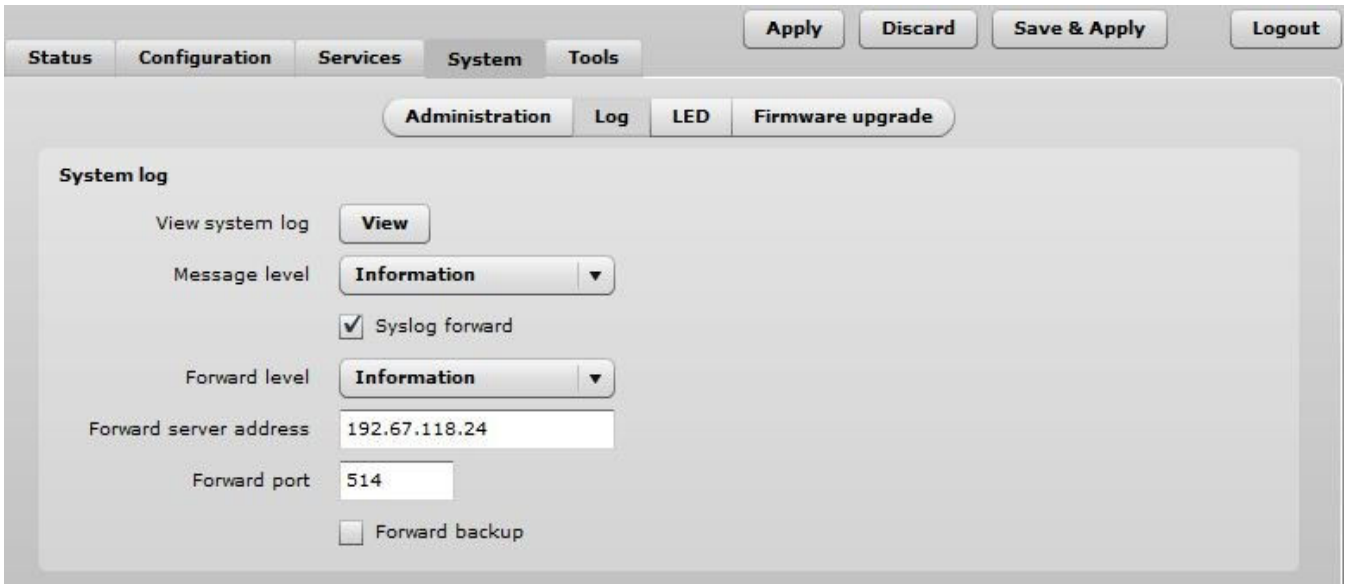
Download troubleshooting file : click to download the troubleshooting file. The troubleshooting file contains valuable information about device configuration, routes, log files, command outputs, etc. When using the troubleshooting file, the device quickly gathers troubleshooting information automatically, rather than requiring you to gather each piece of information manually. This is helpful for submitting problems to the support team.

Backup configuration file : click to save the current configuration file. The saved configuration file is useful to restore a configuration in case of a device misconfiguration or to upload a standard configuration to multiple devices without the need to manually configure each device through the web interface.

Restore configuration from file : click to upload an existing configuration file to the device.

Log

Use the log tab to configure device to view or save log messages to the local or remote server using standard syslog facility:



View system log : click to view current trace messages. The system log viewer utility provides debug information about the system services and protocols. If the device's malfunction occurs recorded messages can help operators to locate misconfiguration and system errors.

Message level : specify system's message tracing level. The level determines the importance of the message and the volume of messages generated by the device. The levels are in increased importance order [emergency, alert, critical, error, warning, notice, information, debug]. Default: info.

? The device can be configured to send system log messages to a remote server:

Syslog forward : select to enable remote system logging.

Forward server : specify the remote host IP address or hostname where syslog messages will be sent.

Forward port : specify the port to which syslog messages will be forwarded [0-65535]. Default: 514.

Forward message level : specify the level of the message which will be sent to the remote syslog server. The level determines the importance of the message and the volume of messages generated by the device. The levels are in order of increasing importance [emergency/alert/critical/error/warning/notice/information/debug]. Default: information.

Forward backup : select to enable remote syslog logging backup.

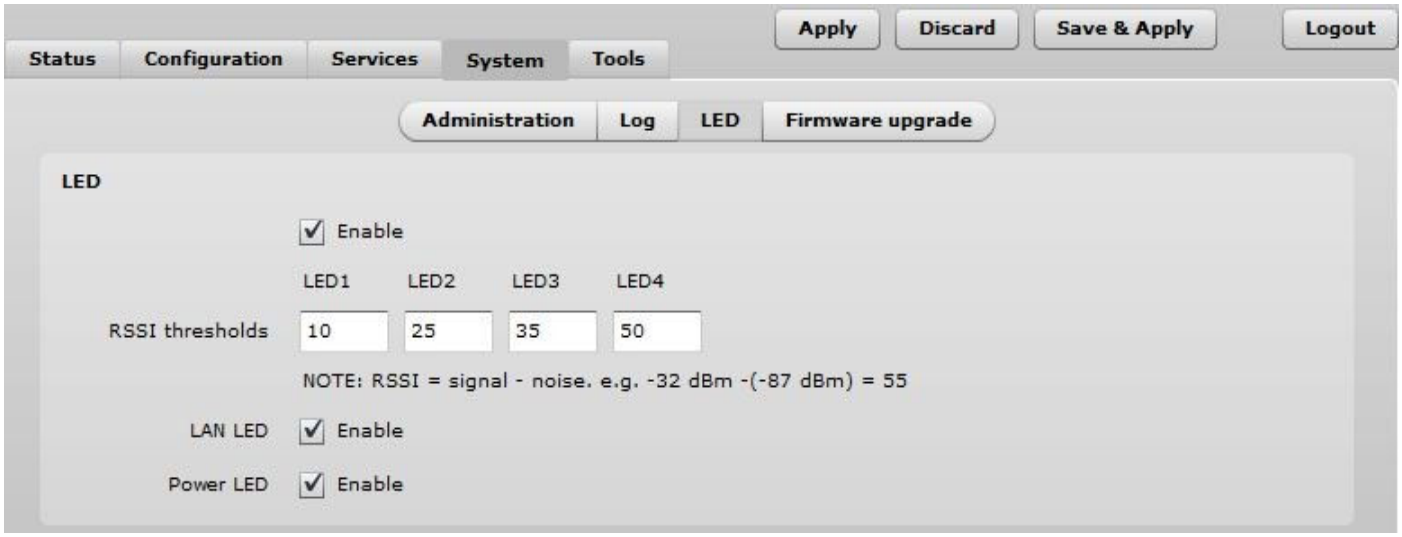
Backup server : specify the backup host IP address or hostname where syslog messages will be send to.

Backup port : specify the port to which syslog messages will be forwarded [0-65535]. Default:

514.

LED Control

The 570n is equipped with 6 LEDs: power, LAN and 4 RSSI LEDs that indicates the signal strength of current connection. The signal level is classified into 4 levels, thus corresponding 4 LEDs switches on as soon as indicated threshold is reached.



Enable : select to enable LEDs on the device. If this option is not selected, then no LED activity will be visible on the device.

RSSI thresholds : specify the RSSI threshold at which corresponding LED will switch on.

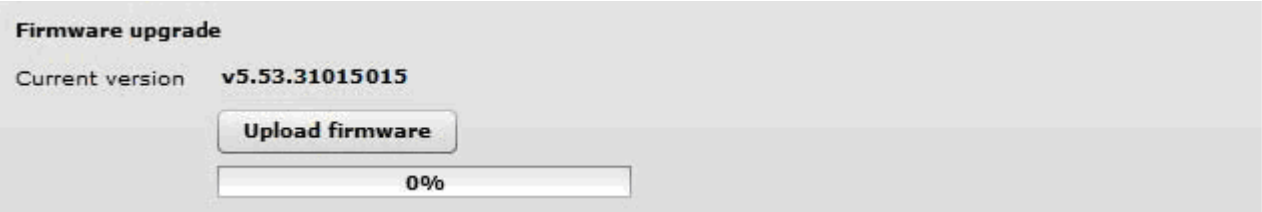
The Signal LEDs are working only when the connection is established. Therefore, please make sure all wireless settings are correct and the connection is established.

LAN LED : select to enable LAN LED. The red LED will be blinking on LAN activity, off : no LAN connection.

Power LED : select to enable Power LED. The steady red LED when power is on, off : no power.

Firmware Upgrade

To update your device firmware use the **System | Firmware** upgrade menu. Press **Upload firmware**, select the firmware file and click the Upload button:



Current version : displays version of the current firmware.

Upload firmware : click the button to select the new firmware image for uploading it to the device.

The device system firmware upgrade is compatible with all configuration settings. When the device is upgraded with a newer version or the same version builds, all the system's configuration will be preserved after the upgrade.

The new firmware image is uploaded to the controller's temporary memory. It is necessary to save the firmware into the device permanent memory. Click the Upgrade button:

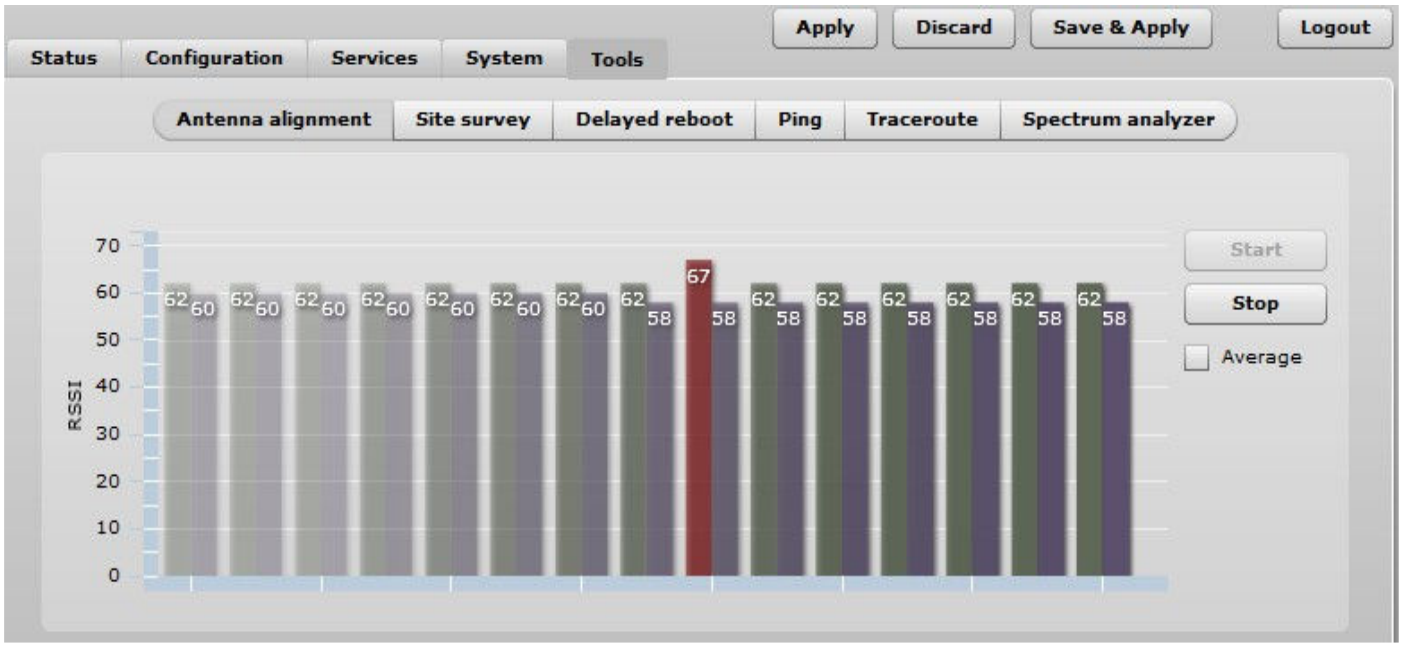
Upgrade : upgrade device with the uploaded image and reboot the system.

Do not switch off and do not disconnect the device from the power supply during the firmware upgrade process as the device could be damaged.

Tools

Antenna Alignment

The **Antenna Alignment** tool measures signal quality between the Station and 570n. For best results during the antenna alignment test, turn off all wireless networking devices within range of the device except the device(s) with which you are trying to align the antenna. Watch the constantly updated display in the Alignment Test window as you adjust the antenna.



Start : press this button to start antenna alignment.

Stop : press this button to stop antenna alignment.

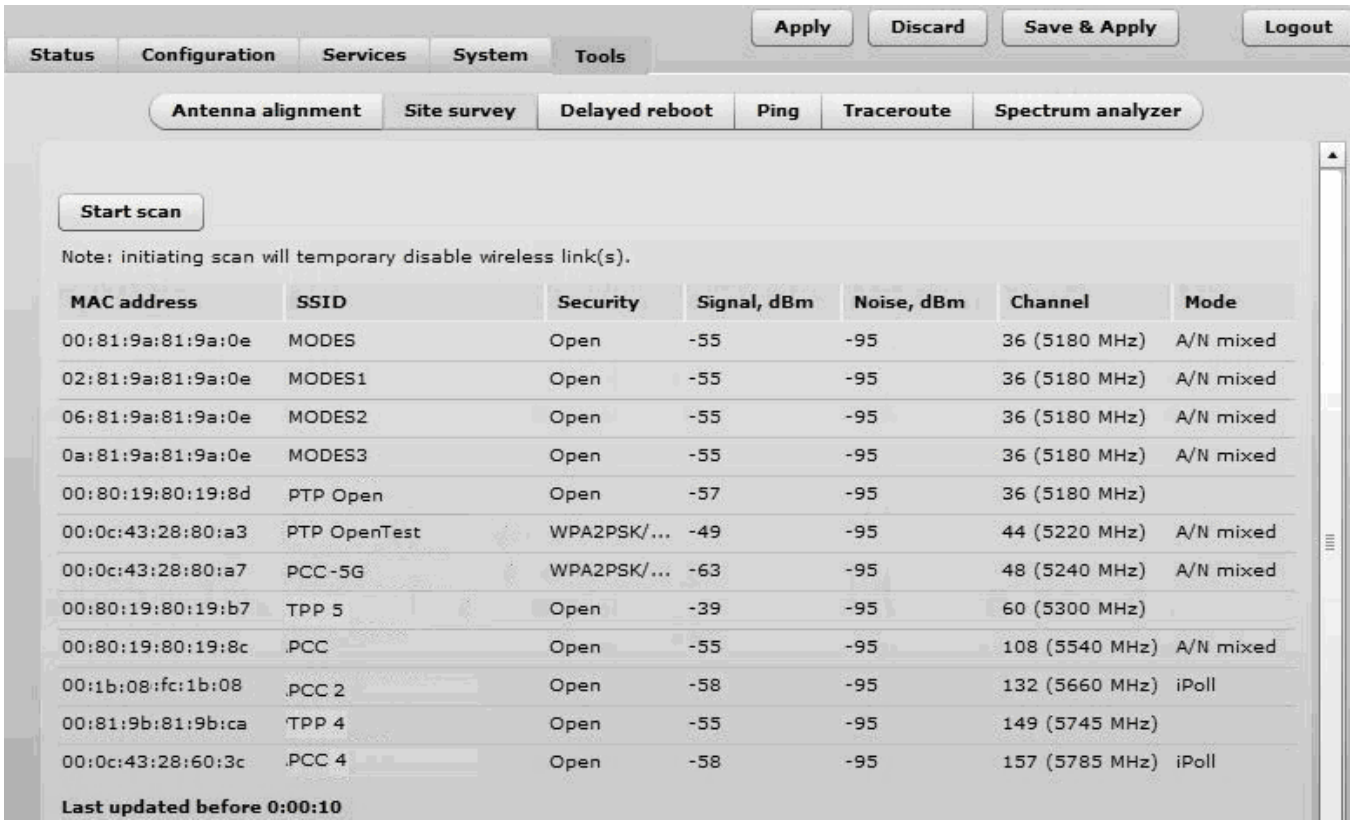
Average : if this option selected, the graph will display the average RSSI of both

antennas.

Site Survey

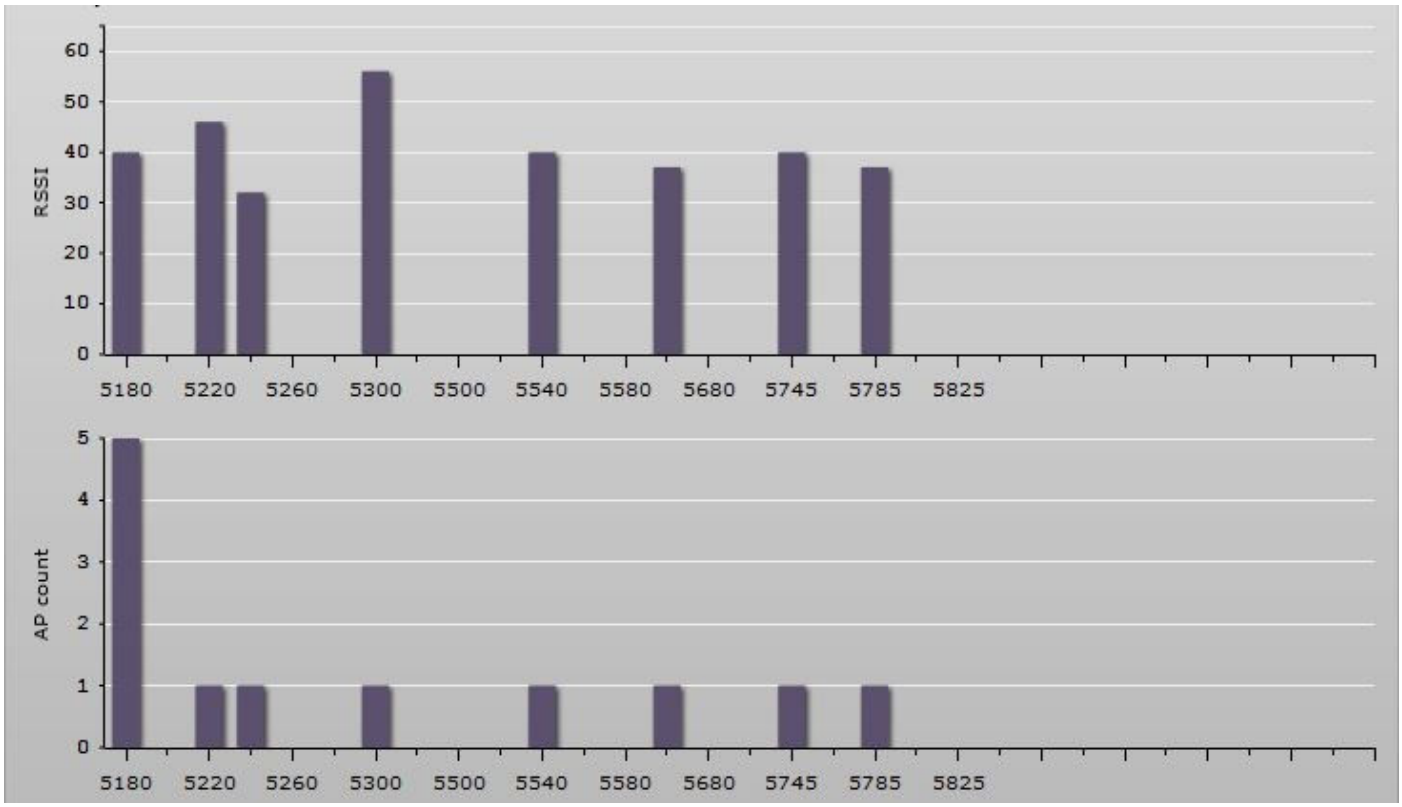
The Site Survey tool shows overview information for wireless networks in a local geographic area. Using this test, an administrator can scan for working access points, check their operating channels, encryption and see signal/noise levels.

To perform the Site Survey test currently, click the **Start scan**:


Apply
Discard
Save & Apply
Logout
Status
Configuration
Services
System
Tools
Antenna alignment
Site survey
Delayed reboot
Ping
Traceroute
Spectrum analyzer
Start scan
Note: initiating scan will temporary disable wireless link(s).
MAC address
SSID
Security
Signal, dBm
Noise, dBm
Channel
Mode
00:81:9a:81:9a:0e MODES Open -55 -95 36 (5180 MHz) A/N mixed
02:81:9a:81:9a:0e MODES1 Open -55 -95 36 (5180 MHz) A/N mixed
06:81:9a:81:9a:0e MODES2 Open -55 -95 36 (5180 MHz) A/N mixed
0a:81:9a:81:9a:0e MODES3 Open -55 -95 36 (5180 MHz) A/N mixed
00:80:19:80:19:8d PTP Open Open -57 -95 36 (5180 MHz)
00:0c:43:28:80:a3 PTP OpenTest WPA2PSK/... -49 -95 44 (5220 MHz) A/N mixed
00:0c:43:28:80:a7 PCC-5G WPA2PSK/... -63 -95 48 (5240 MHz) A/N mixed
00:80:19:80:19:b7 TPP 5 Open -39 -95 60 (5300 MHz)
00:80:19:80:19:8c PCC Open -55 -95 108 (5540 MHz) A/N mixed
00:1b:08:fc:1b:08 PCC 2 Open -58 -95 132 (5660 MHz) iPoll
00:81:9b:81:9b:ca TPP 4 Open -55 -95 149 (5745 MHz)
00:0c:43:28:60:3c PCC 4 Open -58 -95 157 (5785 MHz) iPoll
Last updated before 0:00:10

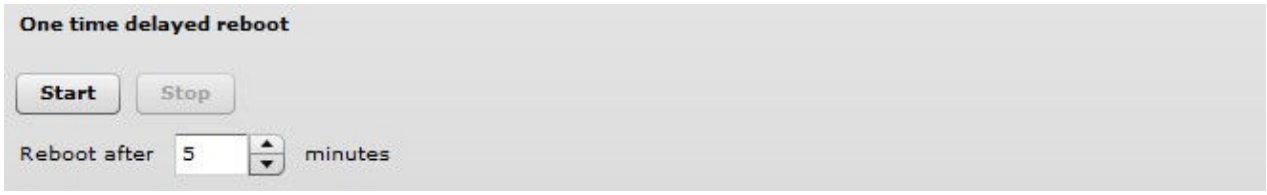
Last updated before : displays when the last scan was performed.

The results of the Site Survey test are converted to handy two graphs: 570n count and RSSI. An administrator can use this to identify the best channel for device operation that will not receive interference from adjacent 570ns.



Delayed Reboot

This tool is extremely useful while tuning radio settings : once you defined hypothetic radio parameters and set them with Apply button (not written to the permanent memory), device starts operating with the new settings, and in case the link fails, device will be rebooted in specified minutes, thus the old settings will be set back.

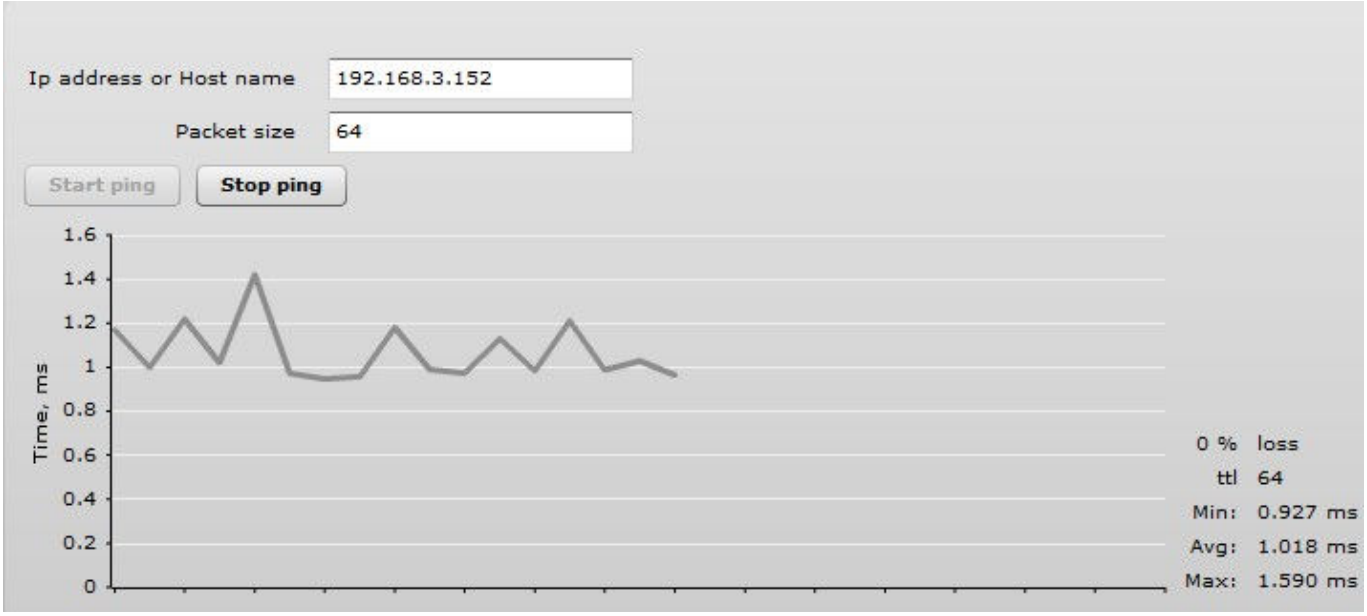


Reboot after : specify time in minutes, after which the device will be rebooted.

Start/Stop : click to start or stop delayed reboot tool.

Ping

This command is used to test whether a particular host is reachable across an IP network. The Ping results will be displayed graphically:

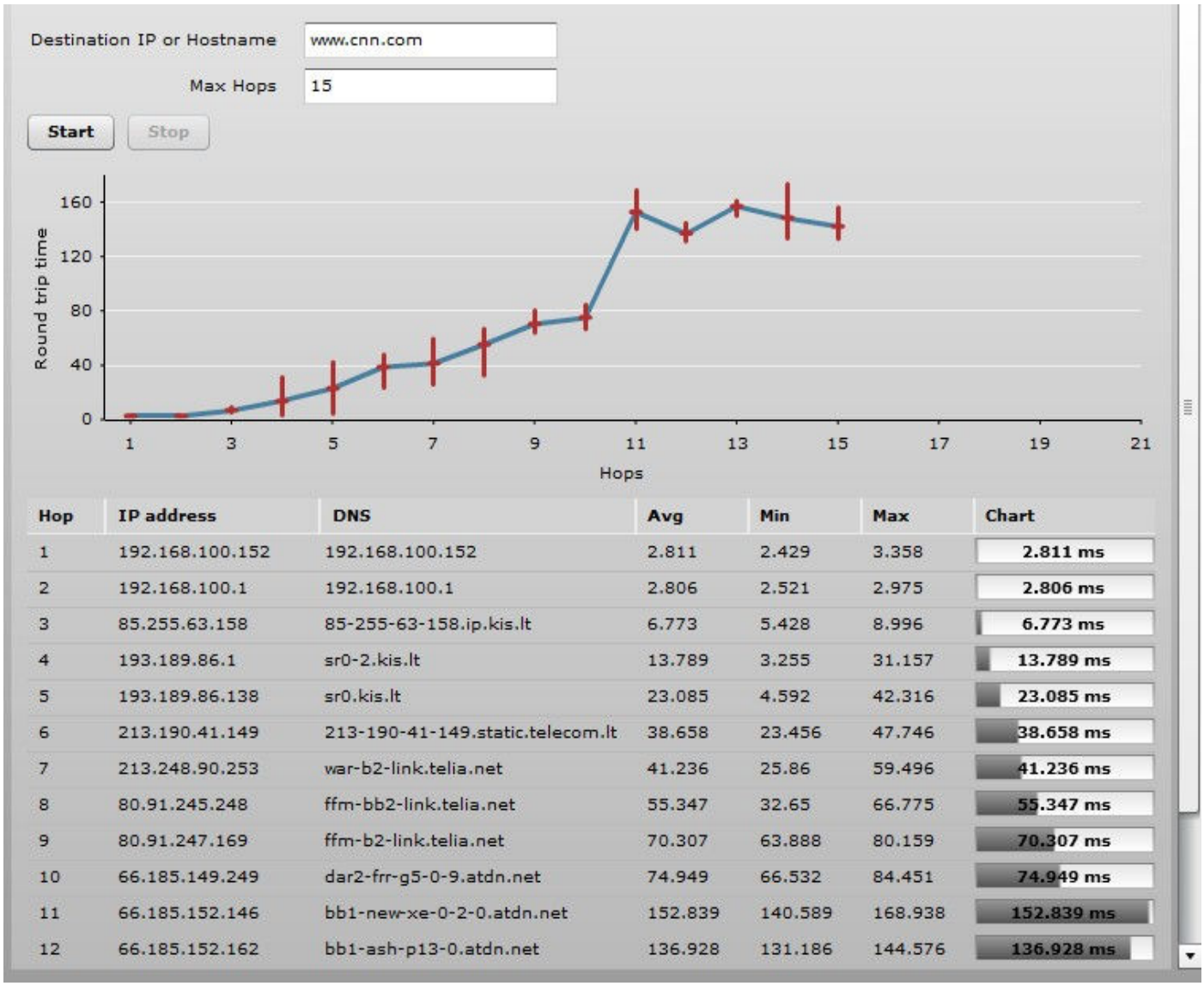


IP address or Host name : specify the destination IP address or Host name.

Packet size : specify the packet size.

Traceroute

This tool is a route-tracing utility used to determine the path that an IP packet has taken to reach a destination. This is useful when trying to find out why destination is unreachable, as you will be able to see where the connection fails.



Hop	IP address	DNS	Avg	Min	Max	Chart
1	192.168.100.152	192.168.100.152	2.811	2.429	3.358	2.811 ms
2	192.168.100.1	192.168.100.1	2.806	2.521	2.975	2.806 ms
3	85.255.63.158	85-255-63-158.ip.kis.lt	6.773	5.428	8.996	6.773 ms
4	193.189.86.1	sr0-2.kis.lt	13.789	3.255	31.157	13.789 ms
5	193.189.86.138	sr0.kis.lt	23.085	4.592	42.316	23.085 ms
6	213.190.41.149	213-190-41-149.static.telecom.lt	38.658	23.456	47.746	38.658 ms
7	213.248.90.253	war-b2-link.telia.net	41.236	25.86	59.496	41.236 ms
8	80.91.245.248	ffm-bb2-link.telia.net	55.347	32.65	66.775	55.347 ms
9	80.91.247.169	ffm-b2-link.telia.net	70.307	63.888	80.159	70.307 ms
10	66.185.149.249	dar2-frr-g5-0-9.atdn.net	74.949	66.532	84.451	74.949 ms
11	66.185.152.146	bb1-new-xe-0-2-0.atdn.net	152.839	140.589	168.938	152.839 ms
12	66.185.152.162	bb1-ash-p13-0.atdn.net	136.928	131.186	144.576	136.928 ms

Destination IP or Hostname : specify hostname or IP address of the target host.

Max Hops : specifies the maximum number of hops to search for target.

Start/Stop : click to start or stop traceroute tool.

Spectrum Analyzer

The Spectrum analyzer test displays detailed information about signal level of each 570n unit's antenna on each available frequency. This enables administrator choose the best available frequency/channel for the unit operation. The frequency list depends on the Country at which the unit is operating, and chosen channel width.

Do not use the Spectrum analyzer on the remote unit of the link, as the connection to the device will be lost during the test.

Click **Start** button to perform the test:

Operating frequency range : displays the channel frequency range at which the 570n unit is operating currently.

Maximum : color indicates a the maximum achieved signal level on the appropriate frequency.

Current : color indicates the current signal level on the appropriate frequency.

Average : indicates average of the signal level on the appropriate frequency.

UAM (Universal Access Method)

UAM authentication is available on radio interfaces (including VAPs) only if 570n is

working as **router** in **Access Point (auto WDS)** wireless mode.

Universal Access Method (UAM) is a simple Web browser based user authentication method. On initial HTTP request to any Web site, client's browser is redirected to the authentication page for login to the network. The login page can be served by internal Web server or by external Web application Server.

UAM Overview

When using internal UAM, the Login page is the first page a client receives when he starts his Web browser and enters any URL. To get access to the network, the user should enter his authentication settings: **Username** and **Password** and click the **Login & Accept Terms** button:

My HotSpot
Welcome to my HotSpot!
You can use the Internet, but have to login first.
You must also agree to these terms and conditions.
Username
Password
Login & Accept Terms

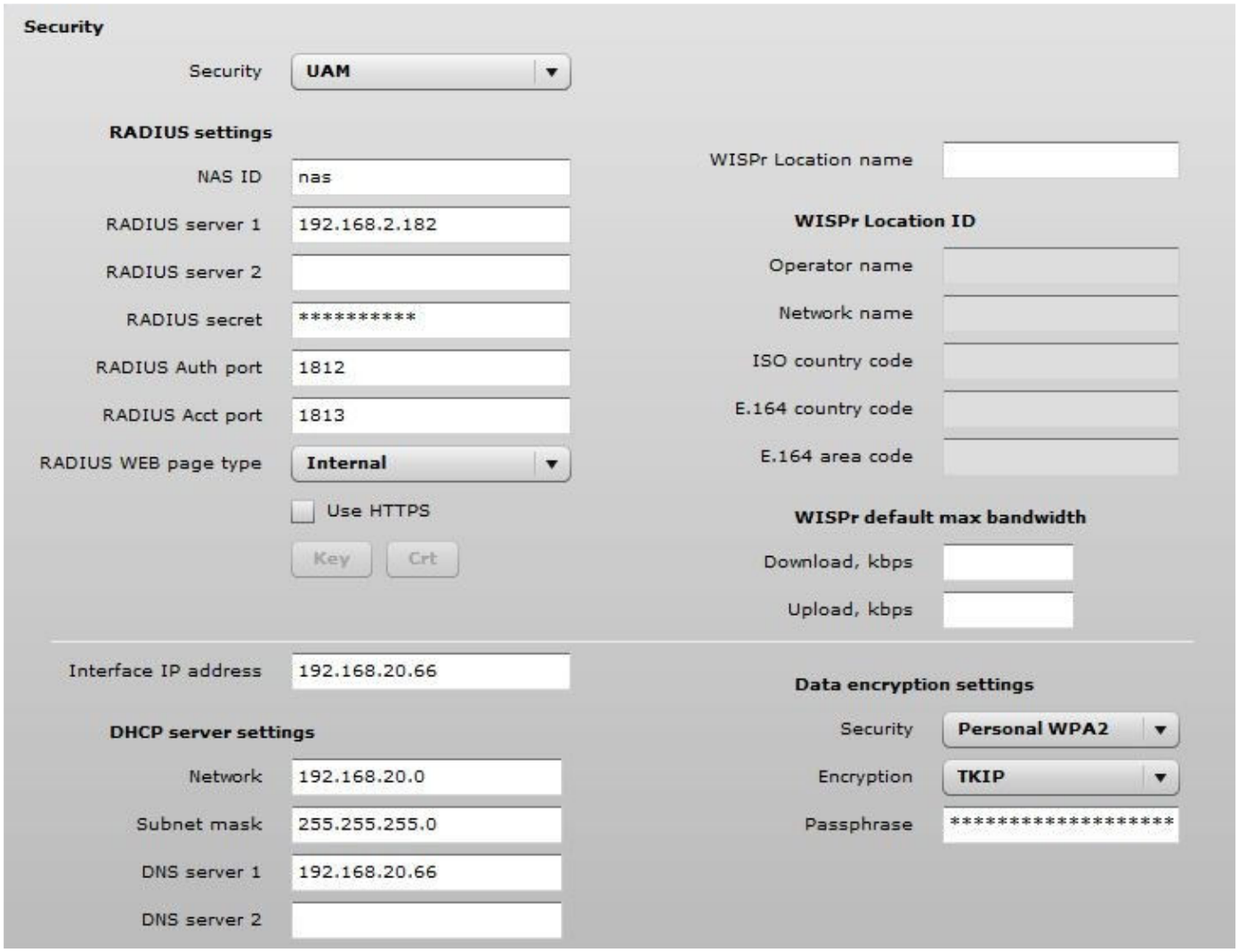
The 570n could be shared by several Wireless Internet Service Providers (WISP). They are uniquely identified by specifying WISP domain name in addition to subscriber user name when logging in.

Subscriber's login format: Username

UAM Configuration

The 570n allows user authentication through external or internal Web portal. This authentication method is called UAM. User provides login credentials and then Web portal attempts to authenticate and authorize the client using the provided information. Client will not send any authentication requests directly to the 570n, the Web portal will do this. On success, 570n will allow access to the Internet; otherwise Web portal will display failure notice.

Use Security section on Wireless or VAP (depending on the interface on which the UAM will be configured) page for UAM configuration: choose the security option UAM:



RADIUS Settings

NAS ID : specify the NAS identifier.

RADIUS server 1 : specify the name or IP address of the primary RADIUS server.

RADIUS server 2 : specify the name or IP address of the secondary RADIUS server.

RADIUS secret : specify the RADIUS shared secret.

RADIUS authentication port : specify the UDP port number to use for radius authentication requests, default 1812

RADIUS accounting port : specify the UDP port number to use for radius accounting requests, default 1813

RADIUS WEB page type : choose the authentication Web portal type:

> **Internal** : use the built in authentication Web page. If selected, then when a users first tries to access the Internet, they will be blocked, and re-directed to the built-in login page. The logon data will be sent to the Radius Server for authentication.
>
> **External** : specify the external authentication Web page URL and settings. If selected, then when a user first tries to access the Internet, they will be blocked, and re-directed to the URL specified below.
>
> **Custom internal** : upload a customized internal page.

Use HTTPS : enable to use the HTTPS protocol for connection and authentication.

> **Key** : upload a PEM formatted private key file.
> **Certificate** : upload a PEM formatted certificate file.

WISPr Settings

> **WISPr location name** : specify the WISPr location name.
> **Operator name** : specify the operator's name
> **Network name** : specify the network name
> **ISO country code** : specify the country code in ISO standard.
> **E.164 country code** : specify the country code in E.164 standard.
> **E.164 area code** : specify the area code in E.164 standard.

WISPr default max bandwidth : specify the default bandwidth limitation for clients. Note that if the external RADIUS server has traffic limitations preconfigured, then RADIUS overrides these settings.

> **Download, kbps** : specify max download bandwidth in kbps.
> **Upload, kbps** : specify the max upload bandwidth in kbps.

Interface IP address : specify the LAN interface IP address. Note that LAN settings on Network menu will be disabled if UAM is enabled. **DHCP settings'** *: specify the dynamic IP settings for*

the connected users:

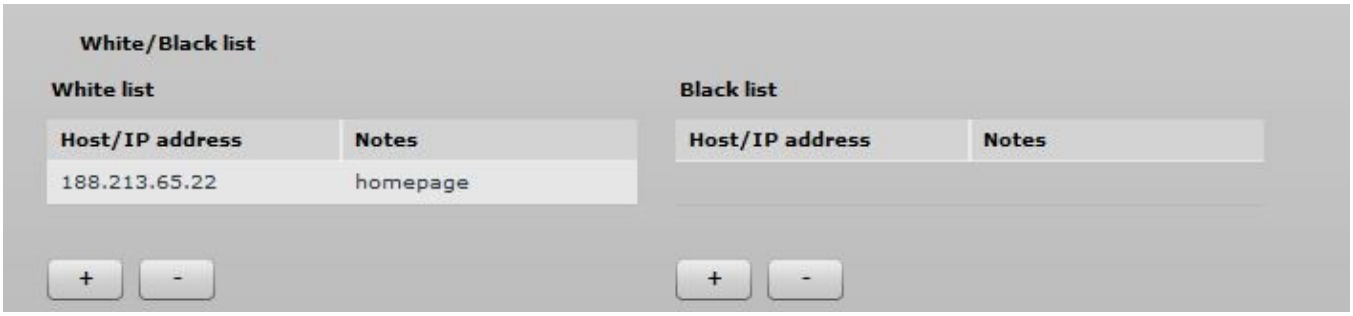
Network : specify the network for IP address pool.
Subnet mask : specify the subnet mask for the DHCP.
DNS server : specify the primary and the secondary DNS servers.

Data encryption settings : choose the data encryption method:

Open : no encryption.
Personal WPA : preshared key encryption with WPA using AES method.
Personal WPA 2 : preshared key encryption with WPA2 using AES method.

White/Black List

The white and black access lists control user access to Web content through the 570n. The unauthenticated users will be allowed to access sites from white list while access to the sites from black list will be denied even for authenticated users.



Use **"+"** sign to add new entry to the list, and **"?"** sign to remove required one.

White list

Host/IP address : specify the IP addresses or hosts for free access even for unauthenticated users.

Notes : add a description for the specified host or IP address.

Black list

Host/IP address : specify the IP addresses or hosts that will be not accessible even for the authenticated users.

Notes : a description for the specified host or IP address.